جمهورية العراق
وزارة التعليم العالي و البحث العلمي
جامعة بابل
كلية القانون

الحماية القانونية للبيانات الشخصية لزبائن الشركات المالية
-دراسة مقارنة-

أطروحة تقدم بها الطالب (الكرار حبيب جهلول) الى مجلس كلية القانون – جامعة بابل

وهي جزء من متطلبات نيل درجة دكتوراه فلسفة في القانون الخاص

بإشراف

أ.د. ميثاق طالب عبد حمادي الجبوري

أستاذ القانون التجاري

1445
2023

﴿إِنَّ السَّمْعَ وَالْبَصَرَ وَالْفُؤَادَ كُلُّ أُولَئِكَ كَانَ عَنْهُ مَسْئُولًا﴾

صدق الله العلي العظيم

سورة الاسراء، الآية (36)

الاهداء

الى الرحمة المهداة للعالمين نبينا محمد واله الهداة الميامين (صلوات الله وسلامه عليهم اجمعين)

الى سكنات روحك التي لم تفارقني ، الى بياض عينيك التي اراها في كل من حولي ، الى انفاسك الطيبة التي ما فتأت تنعشني ، الى قلبك الذي احس بنبضاته في كل نبضة من قلبي .... والدتي عليك من الله رحمة ورضوان .

والدي .. الذي ما بخل علي بعطائه لحظة من لحظات حياتي .

اخوتي .. الذين احبهم من كل قلبي .

زوجتي .. التي تحملت المتاعب في سبيل اكمال هذه المرحلة الدراسية .

حيدر زينب علي .. قلبي النابض وقرة عيني ... اولادي الاحبة .

زملائي في العمل الذين شجعوني دوماً على النجاح

كل من يتصفح هذه الاطروحة

اليهم جميعاً اهدي هذا الجهد العلمي المتواضع

الباحث

شكر وعرفان

اشكر الله سبحانه وتعالى على اعانته وتوفيقه لي في هذه الاطروحة ومن باب اسداد المعروف والشكر الى اهله اتقدم بالشكر الموصول لجناب الاستاذ الدكتور (ميثاق طالب عبد حمادي) الذي شرفني بقبوله ان يكون مشرفا على موضوع الاطروحة ، فكان منه النصح والتوجيه من بداية تنظيم العنوان والخطة الى الانتهاء من الكتابة ، فكان له الاثر الكبير في اخراج هذه الاطروحة ، فجزاه الله خير الجزاء ، واسال الله له الرفعة والعلو ودوام الصحة والعافية ، وان يجعله الله ذخرا للعلم وطلابه .

كما واتقدم بالشكر لأعضاء لجنة المناقشة المحترمون لتجشمهم عناء القراءة وابداؤهم الملاحظات التي تسهم في اخراج الاطروحة بأفضل صورة، فجزاهم الله عني كل خير ، واسال الله ان يجعلني بارا بهم مقدرا جهودهم وفضلهم الكبير .

كما واشكر اساتذتي الاجلاء في جامعة بابل كلية القانون الذين كان لهم الدور الكبير في اكمال هذه المرحلة الدراسية ، فجزاهم الله خير الجزاء .

ولا يسعني الا ان اشكر كل الاساتذة الذين كان لهم الفضل في مسيرتي العلمية في جامعة القادسية اثناء دراسة البكالوريوس ، وفي جامعة كربلاء اثناء دراسة الماجستير ، فلهم مني كل الود ورحم الله المتوفين منهم وحفظ الباقين .

كما يسعدني ويشرفني ان اتقدم بجزيل الشكر ووافر الامتنان الى موظفي المكتبة في كلية القانون جامعة بابل لما ابدوه من مساعدة في البحث عن المصادر والمطالعة في المكتبة ، فلهم كل الاحترام والتقدير .

وفي الختام اود ان اتقدم بعظيم الشكر لزملائي الكرام وذلك لما لمسته منهم جميعا من حسن العشرة ومساعدة وارشاد، فلهم مني عظيم الحب والتقدير، وجزاهم الله خير الجزاء.

الباحث

الملخص

تتمتع البيانات الشخصية والمعلومات بقيمة اقتصادية معتبرة في اطار التعاملات التجارية للشركات في الوقت الحاضر ، حيث تسعى الشركات بوجه عام الى تجميع بيانات الافراد ومعالجتها وتبادلها بما يزيد من ارباحها و منافعها الاقتصادية . شركات مثل تلك التي تسعى الى تقديم الخدمات التعليمية والطبية

او شـركات التواصـل الاجتماعي او الشـركات المالية من المصـارف وغيرها تعتمد في نشـاطها بالدرجة الاساس على التعامل مع البيانات الشخصية للأفراد على المستوى الوطني او الدولي على حد سواء . الا أن هذا النشاط يمكن أن ترافقه اثار سلبية على خصوصية الأفراد وحياتهم الشخصية فضلا عن اثار ذلك على النظام الاقتصادي والاجتماعي للدول.

على هذا الاسـاس عمدت الكثير من المؤسـسـات التشـريعية دولية كانت او محلية الى محاولة تنظيم انتقال المعلومات وتدفقها بطريقة تضمن المنافع الاقتصادية المقصودة منها وتحفظ بالمقابل حقوق الافراد وحياتهم الشـخصـية . الا أن تنظيما من هذا النوع كان محاطا بصـعوبات راجعة الى غياب التنظيم الدولي أولا و طبيعة التعامل مع البيانات وانتقالها الذي غالبا ما يمتد لا كثر من دولة مما يسـتوجب الخضـوع لتنظيمات قانونية مختلفة.

حيث ان اختلاف النظم القانونية وفلسـفاتها المتعلقة بحقوق الانسـان والابعاد الامنية وحتى التجارية تستوجب تنظيما قانونيا عابرا لحدود السلطات القضائية المحلية بما يضمن حماية هذه البيانات وضمان عدم التعدي عليها.

ومن اجل ذلك فرضـت هذه التشـريعات التزامات قانونية على الشـركات المتعاملة بهذه البيانات ، ومنحت حقوق لأصحابها ، وفي حال التعدي عليها او عدم الالتزام بهذه الالتزامات و عدم ضمان الحقوق تتحمل الشركات المسؤولية القانونية، الا في بعض الحالات التي اجاز القانون امكانية افشاءها سواء بسبب طبيعة المعاملة او لأسباب امنية.

المحتويات

المقدمة

أولًا: موضوع الدراسة:

تحتل البيانات مكانة رائدة في مجال النشـــاط الاقتصـــادي لعالم اليوم ، حتى صـــارت المرحلة المعاصـرة تعرف بانها مرحلة اقتصـاد البيانات والمعلومات ، حيث تحظى البيانات ذاتها بقيمة اقتصـادية كبيرة كما انها تمثل أساسـا لأدوات العمل في مجالات الحيات المختلفة ، لا سيما تقنيات الذكاء الصـناعي والروبوتـات والإعلانـات والتجـارة بوجـه عـام . وعلى هذا الأســـاس اجتذبت البيانات اهتمام الشـــركات وحرصـها على الدخول في أنشـطة جمعها أو تخزينها او معالجتها أو نقلها أو غير ذلك مما يمنحها فرصـة الاســـتفادة من المردودات الاقتصـــادية للتعامل بهـا . الا أن البيانـات من جـانـب آخر يمكن ان تحتوي خصـوصـيات من شـأنها ان تعكس المنفعة المقصـودة ضررا أكبر في جوانب حياتية مختلفة لما تحتويه في مكنونها من قدرة التأثير في صـناعة الراي او معرفة الاسـرار والخطط والتوجهات فضـلا عن خطورتها في التأثير على السلم المجتمعي . ومن ابرز ما التفتت اليه التشـريعات المتأخرة من مناطق واجبة الحماية هي موضـوعة البيانات الشـخصية للأفراد ، لا سيما مع انتشار وسائل التواصل الاجتماعي وبرامج البحث وأنظمة الأتمتة للمؤســـســـات الخدمية المختلفة ، حيث تعتمد في نشـــاطها على جمع بينات المتعاملين بها وتخزينها ومعالجتها تمهيدا لنقلها بعمليات تجارية متنوعة ، الأمر الذي يضـــع جانباً مهما من الحياة الشخصية والاجتماعية لأفراد عاديين او غير عاديين في مجال التداول التجاري المحض ويجعلها عرضة للاســـتغلال والاباحة لتوظيفها باتجاهات مختلفة قد تتجاوز في مجال خطورتها النطاق الشـــخصـــي الى مستوى النطاق العام وقد تفوق في ضـررها المنفعة المقصـودة من إدخالها مجال التعاملات الاقتصـادية . وعلى هذا الأساس صدرت التشريعات المتأخرة تأسيساً وتطويراً لنظام حماية البيانات الشخصية وكان من ابرزها صدور اللائحة الاوربية العامة لحماية البيانات الشخصية GDPR رقم ٦٧٩ لسنة ٢٠١٦ ، والتي كان لها تأثيرا عالمياً يتجاوز النطاق الجغرافي او الشـــخصـــي لتطبيق القانون ، الأمر الذي خلف حراكاً تشـريعياً متصـاعداً في العديد من دول العالم كان من ابرزها صـدور قانون حماية البيانات الشـخصـية المصري رقم ١٥١ لسنة ٢٠٢٠ كما أثارت نشاطاً أكاديمياً معتبراً في البحث والنقاش والتدريس وغيرها .

ثانيًا: أهمية الموضوع:

يحظى موضـوع الدراسـة (الحماية القانونية للبينات الشـخصـية لزبائن الشـركات المالية) بأهمية بالغة على المســتويين النظري والعملي على حد ســواء . اذ تتمثل فائدته النظرية بحاجة المكتبة القانونية لدراسة وتحليل ومناقشة التطورات القانونية الناجمة عن فكرة البحث وموضوع الدراسة سواء في ذلك ما ورد في التشـريعات المذكورة أعلاه من تأسـيس لحقوق والتزامات جديدة او ما طرأ على الثابت منها من تطورات تستلزم الوقوف عندها بحثاً ودراسة . واذا كانت تطورات التشريع حالة طبيعية ملازمة لتطورات الأعمال ، فان تطوراً من مثل ما جاء به التشـــريع الأوربي عبر قواعد اللائحة العامة لحماية البيانات الشخصية لسنة ٢٠١٦ يستدعي المتابعة بحثاً للأسس الفلسفية والتطورات النظرية المؤثرة في بناء الأحكام . أما الفائدة العملية فتتمثل أســاســاً في ابراز حالة التطور التشـريعي الملازم لتطورات سـوق العمل وما يشمله ذلك من اظهار الحاجة عملياً لمجاراته وطنياً أو على الأقل تضيق فجوة التنظيم بينما هو محلي وما هو سـائد عالمياً في ظل نظام اقتصـادي عالمي احادي الجانب وأسـواق دولية متداخلة الى حد الاختلاط . يضاف الى ذلك ان موضوع الأطروحة قد اتخذ من الشركات المالية مجالاً خاصاً للدراسة ، وهي شركات تتداخل الأنشطة فيها بحكم الواقع والتخصص وبصرف النظر عن طبيعة النظام القانوني او الاقتصـادي السـائد في دولها التي تنتمي اليها ، لذا يقع على السلطات المعنية بتنظيم عمل الشركات المالية مسؤولية تطوير هياكل العمل والقواعد الخاصـة بممارستها للنشـاط المالي سواء كان ذلك في إطار حراك تشـريعي عام في الدولة ام على مســتوى الشـــركات المالية فقط تجنباً للمســؤولية واعراضـــاً عن طائلة القوانين المستحدثة و المنظمة لحماية البيانات الشخصية.

ثالثًا: إشكالية البحث:

تتمثل الإشـكالية الأسـاسـية للبحث في الأسـس القانوني المعتمدة في إعادة تنظيم المراكز القانونية لأصـحاب العلاقة في التعامل مع البيانات الشـخصـية ، حيث منحت التشـريعات الحديثة الشـخص المعي بالبيانات الشـخصـية سـلطة مطلقة في التصـرف ببياناته وادارتها رغم حيازتها من قبل شـخص آخر (

الشـركة) . اذ أن الحيازة كما هو معروف تمكن الحائز قانوناً من إدارة الشـيء الداخل في حيازته وترتب على أساس ذلك المسؤولية ، بينما كانت الإدارة في اطار تشريعات حماية البيانات الشخصية محل الدراسة لأصحاب تلك البيانات لا على أساس الحيازة المادية لها بل على أساس التصاقها بشخصياتهم وما تمثله من خصوصيات ذاتية واجتماعية لأصحابها ، فرتبت على أساس ذلك حقوقا لأصحاب البينات من قبيل حق الموافقة الصـريحة المجزئة لكل حالة حفظ للبيانات و الحق في النسـيان وغيرها . الأمر الذي يسـتوجب البحث فيما لو كان أساس ذلك راجع في أصله الى القانون ويمتد لفكرة حقوق الانسان ام ان أساسه يرجع الى طبيعة تلك البيانات وخروجها على القواعد المعتبرة في مجال العلاقات القانونية المعتادة . ومن جانب آخر ، يتعرض البحث الى إشـكالية أخرى تتمثل في معالجة التعارض بين حماية الخصـوصـية المتعلقة ببيانات الأشخاص والتزامات الشركات المالية المثبتة دوليا ومحليا عبر تشريعات مكافحة غسيل الأموال وتمويل الإرهاب وغيرها من الانشطة القانونية التي تستلزم الافصاح ، حيث تستلزم الأولى منع الاخرين بوجه عام من الاطلاع على البيانات الشخصية بينما تتطلب الثانية متابعة التحويلات المالية والكشف عن البيانات الشخصية لأصحابها بغية تحقيق اهداف القوانين المعنية . يضاف الى ذلك ان من اهم ما يمر به البحث هو إشكالية التطبيق والنفاذ للائحة الاتحاد الاوربي العامة لحماية البيانات GDPR لسنة ٢٠١٦ ، اذا ان هدفها المعلن يتمثل بحماية بيانات الأشـخاص الاوربيين ، الا أن تطبيق احكامها والعقوبات الناجمة عن مخالفتها يجعل جميع الشـركات والمؤسـسـات المالية في العالم عرضـة لطائلة العقوبات في حال عدم التزامها بالأسس والقواعد التي تضمنتها . وهي حالة من الخروج على النطاق الشخصي والإقليمي لتطبيق القانون فرضتها طبيعة الأنشطة المتداخلة والصفة الاقتصادية السائدة عالمياً على أساس انفتاح الأسواق وتحرير التجارة واعتماد المجال الالكتروني في جميع ذلك ، مما يجعل الشركات المالية في العراق وبلدان المنطقة بوجه عام ملزمة واقعياً بمجاراة أحكام التشريع الأوربي .

رابعًا: نطاق الدراسة:

تتمثل دراسة حماية البيانات الشخصية لزبائن الشركات المالية في التقصي عن ماهية هذه البيانات محل الحماية وصورها وبيان مصدر والية تلك الحماية اضافة الى مظاهر تلك الحماية بالاطار القانوني والاتفاقي ، فضلا عن عرض اهم صور الاعتداء على البيانات الشخصية ، وبيان المسؤولية التي تترتب على التعدي عليها في اطار كل من اللائحة الاوربية لسنة 2016 والتشريع المصري لعام 2020 وغيرهما من القوانين.

خامسًا: منهج الدراسة:

يعتمد الباحث منهج الدراسـة القائم على الوصـف التحليلي المقارن للسـياسـة التشـريعية المتعلقة بالحماية القانونية للبيانات الشـخصـية في كل من اللائحة الأوروبية العامة لحماية البيانات الشـخصـية رقم 679 لسـنة 2016 وبعض تشـريعات دول الاتحاد الأوربي ، والتشـريع المصـري بما فيه قانون حماية البيانات الشخصية المصري رقم 151لسنة 2020 وقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 وغيرها من القوانين المصـرية ، وبعض النصـوص الموجودة في التشـريع العراقي لا سـيما في قانون المصارف رقم 94 لسنة 2004 وكذلك قانون مكافحة غسيل الأموال وتمويل الإرهاب رقم 39 لسنة 2015 وغيرها من التشـــريعات الوطنية ، وذلك من خلال الوقوف على النصـــوص القانونية المختلفة والاحكام القضـائية والاراء الفقهية المختلفة لابراز الحجج والاسـانيد المختلفة المتعلقة بامور الدراسـة ، علما ان الباحث سـيعضـد بعض فقرات اطروحته بنصـوص تشـريعية لقوانين أخرى غي التشـريعات المقارنة ، والتي يرى من وجهة نظره بان فيها فائدة علمية وعملية لموضوع الدراسة .

سادسًا: خطة البحث:

نظرا لاهمية موضـــوع الحماية القانونية للبيانات الشـــخصـــية لدى زبائن الشـــركات المالية ، واعتبارها واحدة من اهم السلع في الوقت الحاضر سيتم تناول الموضوع في ثلاثة فصول حيث سيتناول الفصل الاول ماهية البيانات الشخصية لزبائن الشركات المالية والذي سنقسمه الى مبحثين في الاول نبين مفهوم البيانات الشخصية لزبائن الشركات المالية فيما سنبين في الثاني اهمية البيانات الشخصية في مجال البيئة التجارية وآلية التعامل بها .

ويتناول الفصـل الثاني الاحكام المنظمة للبيانات الشـخصـية بحدود العلاقة بين الشـركات المالية وزبائنها وذلك من خلال مبحثين ، حيث يكون الاول علاقة الشركات المالية بأصـحاب البيانات الشخصية فيما سيكون الثاني الضمانات القانونية لحماية البيانات الشخصية.

بينما يتناول الفصل الثالث المسؤولية المترتبة على انتهاك البيانات الشخصية وذلك في مبحثين ، حسين سيتناول الاول احكام المسؤولية القانونية للشركة المالية فيما سيتناول الثاني القيود المترتبة على قيام المسؤولية.

الفصل الاول

ماهية البيانات الشخصية لزبائن الشركات المالية

تحتل البيانات الشخصية دورا أساسيا في التشريعات الناظمة للعلاقات التجارية بين الزبائن والشركات المختلفة ، اذ ان الأخيرة ومن خلال تعاقداتها مع افراد المجتمع بمختلف طوائفهم وانتماءاتهم تعمد الى طلب جملة من البيانات الشخصية المتعلقة بهم ، ولعل تلك البيانات التي تطلبها شركة ما ، هي ليست بالضرورة نفس البيانات التي تطلبها شركة أخرى ، وقد تكون كلاهما للزبون نفسه مما يترتب على تجميعها إعطاء صورة معينة ومتكاملة عنه وعن توجهاته ومتبنياته التي قد يكون في الغالب غير راغب في البوح بها ، لذا نجد المشرع في اغلب الدول وبالخصوص التشريعات المقارنة ينبري الى حماية تلك البيانات وحظر افشائها ، بيد ان تحديد تلك الحماية ووسائلها وآثارها يستلزم أولا تحديد نطاقها والذي يرتكز في اصله بتبيان مفهوم تلك البيانات ومن ثم تبيان أهميتها وهو ما سنتناوله في المبحثين الاتيين .

المبحث الاول

مفهوم البيانات الشخصية لزبائن الشركات المالية

يعد مفهوم البيانات الشخصية من المفاهيم النسبية المرنة ، بمعنى تغير هذا المفهوم وتبدله بين مجتمعات واخرى وبين الثقافات والموروث الحضاري للدول ، وكذلك بين زمان واخر ، وتطورت البيانات الشخصية مع تطور التكنلوجيا وخصوصا في مجال الانترنت فلم يعد المتاح منها الاسم ، والعنوان البريدي فقط ، بل ازدادت وتنوعت لتشمل صورة الشخص وصوته ، علاوة على طائفة اخرى من البيانات التي تتعلق بقدرته المالية والمعلومات الخاصة بوضعه المالي والشخصي بالكامل ، ولغرض اعطاء فكرة واضحة عن مفهوم البيانات الشخصية لزبائن الشركات المالية لابد من تعريف البيانات الشخصية لزبائن الشركات المالية وتحديد طبيعتها القانونية وبيان نطاقها وهو ماسنتناوله في مطلبين ، في الاول سنتناول تعريف البيانات الشخصية لزبائن الشركات المالية ، وفي الثاني سنبين طبيعتها القانونية وتحديد نطاقها .

المطلب الاول

تعريف البيانات الشخصية لزبائن الشركات المالية

ان مصطلح البيانات الشخصية لزبائن الشركات المالية هو مصطلح مركب من جزئين (البيانات الشخصية) و (زبائن الشركات المالية) ، لذا لابد من تعريف كلا الجزئين بشكل منفرد لنصل الى التعريف الكامل للبيانات الشخصية لزبائن الشركات المالية .

الفرع الاول

تعريف البيانات الشخصية

يعد حق الفرد في السيطرة على المعلومات الخاصة او مستودع اسراره وخصوصياته بجميع اشكالها والحق في الحرية في مواجهة تحديات العصر الرقمي من الحقوق المهمة واللصيقة بشخص الانسان ، ويتم تعريف البيانات الشخصية [1] على انها (سلسلة غير مترابطة من الحقائق الموضوعية التي يمكن الحصول عليها عن طريق الملاحظة او عن طريق البحث والتسجيل ، وتتصف البيانات بكونها صماء اي لا تعبر عن اي اتجاه بل هي بيانات خام اولية لا قيمة محددة لها الا ان تترابط مع بعضها سواء اكانت مجموعة من الحروف او الكلمات او الارقام او الرموز او الصور) .[2]

وذهب البعض في تعريف البيانات الشخصية على انها مجموعة من المعلومات التي تمس الانسان في شخصه وتنتمي الى كيانه كأنسان ، ومن ثم فانها تستخدم في تحديد هوية الفرد ، سواء بشكل مباشر او غير مباشر مثل (الاسم وتاريخ الميلاد ورقم الضمان الاجتماعي والصورة وعنوان البريد الالكتروني)[3] ، الا ان ما يؤخذ على هذا التعريف انه فضفاض ولا يحدد كنه تلك البيانات .

وهناك من عرف البيانات الشخصية بانها (تلك المعلومات التي تمثل عنصرا من الحياة السرية للفرد والتي يضار صاحبها حال افشائها) [4]، وان كان هذا التعريف الاخير اعتمد معيار الضرر لتحديد البيانات الشخصية الا انه ايضا لم يعرفها بشكل واضح ولم يحدد معالمها او يحدد ذاتها .

وهناك من عرفها بانها (هي اي بيانات تتعلق بشخص طبيعي وتحدد هويته بطريقة مباشرة او غير مباشرة ، واي كانت طريقة الحصول عليها سواء من جانب الشخص صاحب البيانات نفسه او الجانب الخاص بأحدى المؤسسات او الجهات الاخرى ، فهي محمية ومصانة ولا يجوز التعرض لها الا للمصلحة العامة وفقا لما تحدده السلطات العامة) [5].

ونحن بدورنا نتفق مع هذا التعريف اذ انه حدد هذه البيانات بشكل كامل ودقيق وبغض النظر عن طريقة الحصول عليها فهي محمية بموجب القانون ولا يجوز التعرض لها وانتهاكها الا على سبيل الاستثناء وبالتحديد بناء على مقتضيات المصلحة العامة ووفقا لما تحدده الجهات المختصة .

اما على مستوى التشريع فلم نجد هناك موقف من المشرع العراقي لتعريف البيانات الشخصية على قدر اطلعنا في هذا الموضوع . بخلاف المشرع المصري والذي تصدى لتعريفها في قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018 ، حيث نص على انه يقصد بالبيانات الشخصية (اي بيانات متعلقة بشخص طبيعي محدد او يمكن تحديده بشكل مباشر او غير مباشر عن طريق الربط بينها وبين اي

---

[1] يتكون مصطلح البيانات الشخصية من مفردتين " بيانات " و " شخصية " لذلك من اللازم في اللغة تعريف كل كلمة على حدة ، وكلمة البيانات في اللغة مشتقة من (بينَ) والبيان اي اخراج الشيء من حيز التجلي ، وما يثبت به الشيء من الدلالة. والشخصية نسبة الى الشخص ، وما تدل مادة الشخص على الظهور والارتفاع حيث ((الشين والخاءُ والصادُ اصلُ واحد يدل على ارتفاع في شيء من ذلك الشخص وهو سواد الانسان اذا سما لك من بُعد)) ينظر محمد بن ابي بكر بن عبد القادر الرازي ، مختار الصحاح ، دار الكتب الحديثة ، الجزء الاول ، 1978 ، ص29 . و احمد بن فارس بن زكريا القزويني الرازي ، معجم مقياس اللغة ، تحقيق عبد السلام محمد هارون ، دار الفكر ، 1979 ، ص254.

[2] د. منى تركي و د. جان سيريل فضل الله ، الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة ، بحث منشور في مجلة كلية بغداد للعلوم الاقتصادية الجامعة ، العدد الخاص بمؤتمرها ، 2013 ، ص5 .

[3] د. عمر احمد حسبو ، حماية الحريات في مواجهة نظم المعلومات ، دار النهضة العربية ، القاهرة ، 2000 ، ص 156 .

[4] د ، حسام الدين كامل الاهواني ، الحق في احترام الحياة الخاصة ، دار النهضة العربية ، القاهرة ، 1978 ، ص61 .

[5] د . باسم محمد فاضل مدبولي ، المسؤولية المدنية عن اضرار معالجة البيانات الرقمية ، دار الفكر الجامعي ، ط1 ، 2020 ، ص20 .

بيانات اخرى) [1]. ثم ما لبث ان عاد المشرع المصري وقام بتعريف البيانات الشخصية بانها (اي بيانات متعلقة بشخص طبيعي محدد او يمكن تحديده بشكل مباشر او غير مباشر عن طريق الربط بين هذه البيانات واي بيانات اخرى ، كالاسم او الصوت او الصورة او الرقم التعريفي او محدد الهوية عبر الانترنت او اي بيانات تحدد الهوية الشخصية، او الصحية او الاقتصادية ، او الثقافية ، او الاجتماعية) [2] وبقراءة النص المصري بشكل متعمق يظهر انه قد اقتصر على البيانات المتعلقة بالاشخاص الطبيعيين فقط ، كما تضمن التعريف للبيانات الشخصية بعض الامثلة التي تبين هوية الشخص مثل الاسم او الصورة او الصوت .... ولكن الامثلة التي وردت بهذه المادة بالنسبة للبيانات الشخصية انما اتت على سبيل المثال وليس على سبيل الحصر ، وهذا يعني ان اي بيانات اخرى من الممكن ان يتم اعتبارها بيانات شخصية طالما تعلقت بشخص طبيعي محدد او من الممكن تحديده . اما اذا كانت هذه البيانات غير متعلقة بشخص محدد ولا توجد اي امكانية لتحديده بشكل مباشر او غير مباشر فانه وبمفهوم المخالفة لنص المادة في تعريفها للبيانات الشخصية لا يمكن اعتبار هذه البيانات بيانات شخصية ، وذلك لان المشرع المصري قد اشترط انه لابد ان تكون البيانات متعلقة بشخص محدد او يمكن تحديده لاعتبارها بيانات شخصية .

كما عرفت اللائحة الاوربية (GDPR) البيانات الشخصية بانها (تعني اي معلومات تتعلق بشخص طبيعي محدد او قابل للتحديد والشخص الطبيعي هو الذي يمكن تحديد هويته بشكل مباشر او غير مباشر وبوجه خاص الرجوع الى محدد لهويته مثل الاسم او اللقب او بيانات الموقع او المعرف عبر الانترنت (عنوان IP او عنوان البريد الالكتروني) او لواحد او اكثر من العوامل الخاصة بالهوية البدنية او العقلية او الاقتصادية او الاجتماعية لهذا الشخص الطبيعي).[3]

ويكاد يتطابق تعريف القانون المصري للبيانات الشخصية مع التعريف الوارد في اللائحة الاوربية ، ومد نطاق تحديد هوية الشخص الى النواحي الصحية او الثقافية او الاقتصادية او الاجتماعية ، بيد ان الاخير توسع بعض الشيء في بيان المسائل الخاصة التي يمكن الاستعانة بها لتحديد هوية الشخص الطبيعي ، وهي تتمثل لاول مرة امور مثل المعلومات الجينية او العقلية ومع هذا جاء التعريف المصري عاما وواسعا ايضا بما يسمح باستيعاب هذه المسائل لتحديد هوية الشخص الطبيعي ، اذ تتميز هذه التعريفات بانها تشمل البيانات التي تحدد هوية الشخص بشكل مباشر او غير مباشر ، فالبيانات الموزعة بقواعد بيانات مختلفة قد لا تدل على هوية الشخص بحد ذاتها ، لكن اذا تم ربطها قد تفصح عن هوية الشخص ، ومن ثم في حال اكتفى النص بحماية البيانات التي ترتبط بصاحبها بشكل مباشر فقط قد يسمح ذلك للعديد من الجهات بالتعدي على بيانات الاشخاص ، خاصة مع تقدم تقنيات جمع البيانات ومشاركتها .

وان كان التعريف الاوربي يتمتع ببعض الخصوصية التي تمكننا من سوق بعض المميزات له وكالاتي :

1- انه يوسع من مدلول مصطلح البيانات الشخصية كما اسلفنا ومن ثم فانه يوفر حماية اكبر للمستخدم ، حيث يؤدي اعمال هذا التعريف الى توسيع تطبيق نطاق هذا القانون ، اما التضييق من مفهوم البيانات الشخصية فقد يؤدي الى الى مزيد من انتهاك الحق في الخصوصية عبر تكنولوجيا

---

[1] انظر المادة (1) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.

[2] انظر نص المادة (1) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[3] انظر نص المادة (4) من اللائحة الاوربية لحماية البيانات الشخصية (GDPR) لسنة 2016 .

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

الانترنت والاتصال ، نتيجة قيام الافراد والشركات والجهات الحكومية بالتعدي على تلك البيانات .

2- ان اللائحة نصت صراحة على اعتبار البيانات التي تحدد هوية الشخص عبر شبكة الانترنت من ضمن البيانات الشخصية ، ومن ثم فان البيانات الشخصية تشمل عنوان البريد الالكتروني ، وعنوان ال (IP) وغيرها من البيانات التي تحدد هوية الشخص عبر شبكة الانترنت . ونتمنى من المشرع العراقي مستقبلا الاخذ بهذا المفهوم في تشريعه المنتظر لقانون يحمي البيانات الشخصية على غرار ماذهب اليه المشرع الاوربي ، حتى لايدع مجالا للاجتهاد في هذه المسألة .

3- ان اللائحة الجديدة نصت صراحة على اعتبار بيانات الموقع ، والمعلومات الوراثية وغيرها من البيانات من ضمن البيانات الشخصية .

وان كان هناك من الفقه [1]من وجه سهام النقد لتعريف البيانات الشخصية واعتبروه موسع للغاية منوهين الى ان التحليلات الضخمة للبيانات من شأنها ان تجعل التفرقة بين البيانات التي تجعل من الشخص قابل للتعريف وتلك التي لا تجعله قابل للتعريف لا قيمة لها [2] .

وذهب القضاء الانكليزي في تعريفه للبيانات الشخصية في حكم له عام (2003) بانه مجرد ذكر شخص صاحب بيانات بوثيقة لدى المتحكم لا يعد بالضرورة من قبيل البيانات الشخصية ، وان البيان لا يعتبر شخصي الا اذا كان من شأنه ان يؤثر على حق صاحبه في الخصوصية في اي جانب من جوانب حياته سواء كانت الشخصية او العملية [3].

ويلاحظ ان هذا التعريف يشترط في البيان حتى يكون شخصيا ان يكون من شأنه ان يؤثر على الخصوصية بأن يفصح عن معلومة لايرغب صاحبها في الافصاح عنها سواء كانت تتعلق بحياته الشخصية كالاسم او الصورة او الديانة وغيرها او تؤثر في حياته العملية كالمهنة والدخل والثروة والبريد الالكتروني وغيرها من البيانات التي تتعلق بالخصوصية ، وهو ما يعني من ان تعريف البيانات يعد بمثابة معيار يمكن عن طريقه تحديد ما اذا كانت المعلومة تعد بيانا شخصيا ام لا ، ومن خلال هذا السرد للتعريفات الفقهية والقانونية والقضائية نستطيع تعريف البيانات الشخصية بانها (البيانات الخاصة بالشخص الطبيعي ، والتي تحدد بشكل مباشر او غير مباشر هويته او عناصر حياته او ميوله او معتقداته الدينية او اتجاهاته السياسية او الاجتماعية او الثقافية او عاداته الشخصية او معاملاته المالية او الاقتصادية).

---

[1]Nadezhda Purtova (2018), the law of everything Broad concept of personal data and future of Eudata protection law, Innovation and technology,10:1,40-81, Dol :1001080,17579961020180145217 6, p.30.

[2]Otene and polonetsky, Big Data for All! Privacy and User control in the Age of analytics(2013) 11 NorthWestern Journal of Technology and Intellectual property 258, pp.19_20.

[3]Durant V Financiql Serrices Authority {2003} EWCA Civ 1746 (08 December 2003) /ew/cases/EWCA/civ/2003/1746 http://www.bqilii.org

وتجدر الاشارة الى ان التشريعات تقصر مصطلح البيانات الشخصية على البيانات العائدة للاشخاص الطبيعيين كما اسلفنا ومن ثم فالبيانات الخاصة بالشخص المعنوي مستبعدة من نطاق الحماية القانونية .[1] وهو ما اكدته التشريعات المنظمة للبيانات الشخصية كالمادة الاولى من قانون حماية البيانات الشخصية المصري بقولها " يعمل باحكام هذا القانون والقانون المرافق في شأن حماية البيانات الشخصية المعالجة الكترونيا جزئيا او كليا لدى حائز او متحكم او معالج لها ، وذلك بالنسبة للاشخاص الطبيعيين "ويجب ان لا نقع في الخلط بين مصطلح البيانات الشخصية الذي بينا تعريفه فيما تقدم ومصطلح حماية البيانات الشخصية والذي يشير هذا الاخير الى مطالبة الاشخاص بان لا تكون البيانات الخاصة عنهم متوفرة تلقائيا لغيرهم من الافراد او المنظمات ، حتى في حالة كون البيانات مملوكة من طرف اخر ، فلهم القدرة على ممارسة قدر كبير من السيطرة او التحكم بتلك البيانات وطريقة استخدامها [2].وعلى ذلك عرفها البعض بأنها (حق الافراد في التحكم في بياناتهم الشخصية وتحديد الاشخاص المسموح لهم بالاطلاع على تلك البيانات ، وكيفية التعامل معها ، وقدرتهم في اي وقت على الوصول اليها وتعديلها وتصحيحها وحذفها) [3].

وايضا كثيرا ما تستخدم البيانات الشخصية كمرادف للمعلومات رغم الاختلاف بينهما في المعنى والمفهوم والدلالة ، اذ تعرف المعلومات بانها (مجموعة من الرموز والحقائق او المفاهيم او التعليمات التي لا تصلح لان تكون محلا للتبادل والاتصال او التفسير او التأويل او المعالجة بواسطة الافراد او الانظمة الالكترونية وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها او نقلها بوسائل متعددة)[4].

اما البيانات فتعني (تحليل وتفسير المعلومة وذلك بمعالجتها الكترونيا بغرض تمكين ذوي الشأن من الحكم على الظواهر والمشاهدات) [5].

واذا كان لابد من التفريق بين البيانات الشخصية والحق في الخصوصية ، فالخصوصية تعني بشكل أساسي(المحافظة على السرية ومنع التدخل فيما يعتبر حميمية الشخص واسراره عبر حماية البيانات الشخصية بشكل يمنع انتشار المعلومات التي تكشف الحياة الخاصة او تعرضها للانكشاف) [6].

وقد اثير مفهوم خصوصية البيانات الشخصية في الفقه لاول مرة كمفهوم مستقل وذلك في اواخر ستينات واوائل سبعينات القرن الماضي ، وهناك من ذهب الى ان المقصود بخصوصية البيانات هو (حق الاشخاص في تحديد متى وكيف تصل المعلومات الخاصة عنهم للاخرين) [7]. في حين ذهب اخرون

---

[1] د . سامح عبد الواحد التهامي ، ضوابط معالجة البيانات الشخصية ، بحث منشور في مجلة الحقوق الكويتية ، كلية القانون الكويتية ، السنة الثالثة ، العدد التاسع ، 2015 ، ص401-402 .

[2] د. منى تركي الموسوي وجان سيريل فضل الله ، مصدر سابق ، ص5 .

[3] محمود محمد محمد ابراهيم فياض ، المسؤولية المدنية الناشئة عن استخدام تكنولوجيا الاعلام والاتصال ، اطروحة دكتوراه مقدمة الى جامعة المنصورة – كلية الحقوق ، 2018 ، ص 66 .

[4] د. محمد محمد القطب مسعد ، الحماية المدنية للمعلومات الشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال والتواصل ، بحث منشور في مجلة البحوث القانونية والاقتصادية ، تصدر عنِ كلية الحقوق جامعة المنصورة ، العدد 67 ، 2018 ، ص805.

[5] د. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، 2008 ، ص 101 .

[6] د. خالد حسن احمد ، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية ، دار المتب والدراسات العربية ، 2020 ، ص55 .

[7]

بخصوص ذلك الى المعلومات المتعلقة بحالة الشخص الخاصة جدا ، واعتبر ان الشخص يكون متمتعا بالخصوصية المعلوماتية في حالة العزلة والالفة والتخفي [1].

ويتجه رأي في الفقه إلى أن (حماية البيانات الشخصية تعد جزءا من حماية الحياة الخاصة) [2]

وذلك على أساس أن البيانات الشخصية عنصر من عناصر الحياة الخاصة ، فأي معلومة تتعلق بشخص طبيعي تعد بيانا شخصيا وتدخل في إطار الحياة الخاصة له.

في حين يتجه رأي آخر إلى أن حماية البيانات الشخصية لا تدخل كلها في إطار حماية الحياة الخاصة [3]" وذلك على أساس أن البيانات الشخصية ليست كلها من عناصر الحياة الخاصة للفرد" إذ إن هناك بعض البيانات الشخصية تعد من عناصر الحياة الخاصة وهناك بيانات أخرى لا تعد كذلك .

ويعتقد الباحث رجاحة الرأي الثاني ؛ وذلك لأن مفهوم البيانات الشخصية – وفقا للتعريف الجديد في القوانين محل المقارنة "أى معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحدب هويته " ، ومن ثم فلا يمكن القول إن كل المعلومات التي تتعلق بشخص طبيعي هي من عناصر الحياة الخاصة له، فهناك معلومات تتعلق بالشخص الطبيعي ولا تدخل في إطار الحياة الخاصة مثل المعلومات المتعلقة بمهنة الشخص وحرفته. ولعل ذلك ما دفع المشرع في كثير من الدول إلى أن يضع تشريعا خاصا بحماية البيانات الشخصية بعيدا عن حماية الحياة الخاصة[4]

وايضا تخرج من اطار هذا البحث البيانات الحساسة والتي تعرف بانها فئة من البيانات الشخصية ذات نطاق اضيق من نطاق البيانات الشخصية بشكل عام [5]. وتحظر غالبية القوانين جمعها نظرا لارتباطها المباشر بحقوق الانسان والحريات الاساسية التي تقررها المواثيق الدولية [6]، فهذه البيانات بحسب ما يعرفها البعض (كل معلومة تكشف العرق والاثنية والمعتقدات الفلسفية والدينية والاراء السياسية والنشاطات النقابية والصحة) [7]. وبناء عليه نلاحظ بان هذه البيانات ترتبط بحرية المعتقد ومنع التمييز

---

[1] د . فريد جبور ، حماية البيانات الشخصية ، مقال منشور على الموقع الالكتروني التالي
http://lita-Ib.org/archive/56-questions-answers-html, تاريخ الزيارة في 2022/10/18

[2] - Sabine Lipovetsky et Audry Yayon-Dauvet, Le devenir de la protection des données personnelles sur internet, Gaz. pal, 12,13 septembre 2001, 121?? année, nQ 255 à 256, p 2.

[3] يحيى صقر أحمد صقر، حماية حقوق الشخصية في إطار المسؤولية التقصيرية، دراسة مقارنة ، رسالة دكتوراه ، كلية الحقوق - جامعة القاهرة ، 2006، ص 443 .

[4] الولايات المتحدة الأمريكية : قانون حماية البيانات لعام 1997 ، السويد: قانون حماية البيانات الشخصية لعام 1998 ، ألمانيا: قانون حماية البيانات لعام 2000 ، النمسا: القانون الفيدرالي لحماية البيانات لعام 2000 ،فرنسا : قانون حماية البيانات الشخصية الفرنسي 2004 .

[5] د. محمد محمد القطب مسعد ، المصدر نفسه ، ص 806 .

[6] كما هو الحال في المادة 9 من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
كما اشارت الى هذا المنع المادة الثامنة من قانون المعلوماتية الفرنسي رقم 78 لسنة 1978 المعدل باحكام القانون رقم 1321 لسنة 2016 .

[7] د. محمد احمد المعداوي ، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي ، بحث منشور في مجلة كلية الحقوق جامعة بنها ، العدد 33 ، الجزء الرابع ، 2016 ، ص 1947.

وحرية الرأي . بالنظر إلى هذه النصوص نجد أن البيانات الشخصية مفهوم ينسحب تماماإلى المحيط الشخصي وليس الخاص كما يرى البعض ،[1] فالخصوصية تنبني على طبيعة موضوع البيانات فيما لو كانت خاصة وتوصف حينئذ بالبيانات الحساسة كالديانة أو المعتقد والحالة الاجتماعية، وفي هذه المناسبة أكدت محكمة النقض الفرنسية في حكمها الصادر سنة 2014 بأن إدراج الاسم واللقب في محركات البحث من أجل تحسين مرجعيته لا يشكل انتهاكاً للخصوصية أو للبيانات الشخصية ما لم ترتبط ببيانات شخصية أخرى ،[2]ونص كل من المشرع المصري واللائحة الاوربية لحماية البيانات الشخصية على منع معالجة هذه البيانات وعدم جواز التعامل بها [3]

الفرع الثاني

تعريف الشركات المالية

لتحديد مفهوم الشركة المالية بشكل دقيق [4] لابد من تعريفها بكونها شركة اولا والتي تعرف بانها (عقد يلتزم به شخصان او اكثر بان يساهم كل منهم في مشروع اقتصادي بتقديم حصة من مال او من عمل لاقتسام ما ينشأ عنه من ربح او خسارة) [5] .

ويلاحظ على تعريف المشرع العراقي بأنه يبدأ بعبارة عقد وكأي عقد اخر فانه يتطلب اركان معينة لانعقاده ، وايضا باعتبار ان هذا العقد ينشأ شخصا قانونيا مستقلا لابد ان تكون هناك اجراءات ومستلزمات لتأسيس هذه الشركة لا داعي للخوض في غمارها في هذا البحث كون الموضوع اشبع بحثا . وايضا الهدف من هذه الشركة هو تحقيق الارباح واقتسامها وكذلك توزيع الخسائر على الشركاء وتحمل اعباءها ، وما دمنا نتكلم عن الشركات المالية وهي تجارية بطبيعة الحال وحسب ما يذهب إليه المشرع العراقي في قانون التجارة[6]، ونظرا لخطورة وحساسية هذه الشركات فرض المشرع رقابة صارمة عليها واخضعها الى اجراءات معقدة وفرض عليها ضمانات قانونية كبيرة حماية للافراد المتعاملين معها (الزبائن) . لم يذكر المشرع العراقي الشركات المالية وانما ذكر المؤسسات المالية وعرفها في اكثر من

---

[1] د. د.شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لحق الإطلاع على البيانات الشخصية- دراسة مقارنة،دار الفكر والقانون ، الطبعة الأولى، المنصورة،2015 ، ص 41 .

[2]Cour de cassation, 1ère chambre civile, arrêt du 10 septembre 2014.

[3] انظر نص المادة الاولى من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 ، والمادة الرابعة من اللائحة الاوربية لحماية البيانات الشخصية لسنة 2016 .

‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future, ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

[4] تعريف الشركة في اللغة من الشرك الذي هو الاختلاط ، والشركة والشراكة سواء وهي مخالطة الشريكين ، يقال اشتركنا بمعنى الاشتراك ، وقد اشترك الرجلان تشاركا وشارك احدهما الاخر .

والمالية نسبة الى المال وهو من المول وهو الملك ، ذو المال معروف ماملكته من جميع الاشياء ، والمال في الاصل ما يملك من الذهب والفضة ثم اطلق على كل مايقتنى ويملك من الاعيان ، واكثر مايطلق المال عند العرب على الابل لانها كانت اكثر املاكهم ، انظر محمد بن مكرم بن علي ابو الفضل جمال الدين ابن منظور الانصاري ، لسان العرب ، دار صادر ، بيروت ، ط3 ، 1414 ، ص448 .

[5] انظر نص المادة (1/4) من قانون الشركات العراقي رقم (21) لسنة 1979 المعدل .

[6] نص المادة (5) من قانون التجارة العراقي على انه "تعتبر الاعمال التالية اعمالاً تجارية اذا كانت بقصد الربح، ويفترض فيها هذا القصد ما لم يثبت العكس: ثالث عشر: عمليات المصارف. رابع عشر: التأمين"، كما نصت المادة (6) منه على انه " يكون انشاء الاوراق التجارية والعمليات المتعلقة بها عملاً تجارياً بصرف النظر عن صفة القائم بها ونيته".

قانون ، فقد عرفها بانها (المصـرف المرخص او اية مؤسـسـات مخولة بالتعامل بالتحويلات المالية وفق احكام القانون) [1]. وكان الاولى بالمشرع ان يعرفها كونها شركة ، كما انه قصرها على ما يحتاجه قانون التوقيع الالكتروني دون ان يعطي معنى عام للشركة المالية ، اذ انه قصر انواع المؤسسات المالية على المصـارف وشـركات التحويل المالي فقط في حين انه توجد انواع اخرى للشـركات المالية كما بيناه فيما سبق.

وجديرا بالذكر ان المشرع العراقي قد تدارك هذا القصـور في تعريف المؤسسـة المالية وبيان انواعها في قانون مكافحة غسـيل الاموال وتمويل الارهاب رقم (31) لسـنة 2015 فقد عرفه في المادة (1/ ثامنا) المقصـود بالمؤسـسـة المالية " اي شـخص طبيعي او معنوي يزاول نشـاطا او اكثر من العمليات التالية لصـالح احد العملاء او نيابة عنه ، ..... [2]" ، وسـرد مجموعة من الاعمال التي تدخل في صـلب نشـاط الشركات المالية ،وان كان المشرع اشار الى الشخص الطبيعي في تعريفه الا انه لم يكن موفقا في ذلك ، فمن المعلوم ان ممارسـة الاعمال التي تضـطلع بها الشـركات المالية وان كان المشـرع العراقي تلافى النقص الذي اعتراه في تعريفه للشـركات المالية في قانون التوقيع الالكتروني والمعاملات الالكترونية وعدد الاعمال التي تدخل ضمن نشاط المؤسسات المالية وحتى تعدداه لهذه الاعمال لا يعتبر على سبيل الحصر وانما من الممكن اضافة اعمال جديدة مستقبلا وحسب تطور الحياة .

وان المشـرع العراقي اشـترط على بعض الشـركات المالية التي تمارس انشـطة اسـتثمارية في العراق ان تتخذ شـكلا خاصـا وهو الزامية ان تكون على شـكل شـركة اموال (مسـاهمة كما في المصـارف [3] ، او شركة محدودة كما في شركات التحويل المالي) [4] ،بعد ان كان قبل التعديل يشترط ان تكون جميعا على شـكل شـركة مسـاهمة وهذا ما يلاحظ من خلال نص المادة (10/ثانيا) من قانون الشـركات العراقي رقم (21) لسـنة 1997 المعدل ، اذ نصـت على انه يجب ان يأخذ شـكل شـركة مسـاهمة من يمارس اي من النشـاطات الاتية (التأمين واعادة التأمين ، الاسـتثمار المالي) ، والشـركة المسـاهمة كما هو معروف تعد النموذج الامثل لشـركات الاموال اذ انها تتضـمن كافة الاحكام القانونية الدقيقة المتعلقة بشـركات الاموال وتعرف بانها (شركة تتالف من عدد من الاشخاص لايقل عن خمسة يكتتب فيها المساهمون ، باسهم في اكتتاب عام ويكونون مسؤولين عن ديون الشركة بمقدار القيمة الاسمية التي اكتتبوا بها)[5].

ونلاحظ هذا الانشطة التي اشترط القانون في ان تكون عبارة عن شركة مساهمة هي في حقيقتها شركات مالية بحسب طبيعة النشـاطات التي تمارسـها ، اما الشـركات التي تمارس النشـاط المصـرفي في العراق فيجب ان تتخذ شـكل شـركة مسـاهمة عراقية ، وبأن لا تقل نسـبة الاسـهم الاسـمية عن 30% من مجموع اسهم المصرف والقسم الباقي يمكن طرحه في سوق العراق للاوراق المالية [6]. وتعرف المصارف بانها

---

[1] انظر نص المادة (1) من قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (78) لسنة 2012 .

[2] انظر نص المادة (1/ثامنا / ه) من قانون مكافحة غسيل الاموال وتمويل الارهاب رقم (39) لسنة 2015 .

[3] وبهذا انسجم قانون الشركات العراقي مع الاتجاه العام للقوانين محل المقارنة ، فقد نصت المادة الاولى من قانون شركات الاستثمار الفرنسي الصادر عام 1945 والمعدل في 1957 في باب الشركات الوطنية للاستثمار بانه " يجوز لوزارة المالية الترخيص بانشاء شركات وطنية للاستثمار متى ما اتخذت شكل شركة مساهمة . وكذلك فقد اشترط المشرع المصري في قانون توظيف الاموال رقم 146 لسنة 1988 وفي المادة الاولى منه " ان تتخذ شركة الاستثمار شكل شركة مساهمة ذات اكتتاب عام ، ويسجل في السجل الخاص الذي يوجد في الهيئة العامة لسوق المال .

[4] انظر نص المادة (2) من التعليمات رقم 8 لسنة 2015

[5] انظر نص المادة (1/6) من قانون الشركات العراقي رقم (21) لسنة 1997 المعدل .

[6] انظر نص المادة 1/رابعا /أ من دليلي العمل الرقابي الصـادر من البنك المركزي العراقي بالكتاب رقم 136/2/9 في 2019/4/1 .

(شخص معنوي يتمتع بالشخصية القانونية والاستقلال المالي وهو يعتبر تاجرا في علاقاته مع الغير ، ويجري عملياته وينظم حساباته وفقا للقواعد التجارية المصرفية ، والعرف التجاري المصرفي) [1] .
وعرف المشرع العراقي المصرف بكونه (شخصا يحمل ترخيصا او تصريحا بمقتضى هذا القانون لمباشرة الاعمال المصرفية بما في ذلك شركة حكومية منشأة وفق قانون الشركات الحكومية المرقم (22) لسنة 1997)[2] ، في حين عرف بعض الفقه المصارف بانها (مؤسسات مالية وسيطة تسهل عملية العرض والطلب على النقود ، فيقوم من لديه فائض من الثروة يزيد عن حاجته بالاحتفاظ به في المصرف ، ثم يقوم المصرف باقراض الشخص الذي يحتاج لسيولة او مبلغ معين من المال ما يحتاجه مقابل ضمان او اصل ثابت يساوي او يزيد على قيمة المبلغ المقترض) [3].

اما شركة الاستثمار المالي فقد تبناها المشرع العراقي لاول مرة في قانون الشركات النافذ وعرفها بكونها "

(شركة منظمة في العراق نشاطها الرئيسي فيه توجيه المدخرات نحو الاستثمار في الاوراق المالية العراقية بما في ذلك الاسهم والسندات وحوالات الخزينة والودائع الثابتة) [4]. فهي اذا شركات مالية هدفها الرئيس تمكين المدخرين والمستثمرين من دمج الاموال التي لديهم مع اموال الغير ، لاستثمارها في انواع اخرى من سندات واسهم الاستثمار ، او استثمار قسم من اموالها في شركات اخرى وفق احكام القانون .كما نص القانون ايضا على انه (تعتبر شركة الاستثمار المالي من المؤسسات المالية الوسيطة لاغراض قانون البنك المركزي المرقم 64 لسنة 1976 ، ويعتبر البنك الجهة القطاعية المختصة بنشاطها ويمارس سلطة الرقابة والاشراف عليها)[5] . وان كان قد علق العمل بقانون البنك المركزي العراقي رقم 64 لسنة 1976 بموجب امر سلطة الائتلاف المنحلة رقم 56 لسنة 2004 المعدل ، حيث ان هذا الامر قد علق المادة 18 التي كانت تنص على ان البنك المركزي الجهة القطاعية المختصة بنشاط شركات الاستثمار المالي ، في حين ابقى المادة (9/ثانيا) التي نصت على ان البنك المركزي هو الجهة القطاعية المختصة بنشاط هذه الشركات ويمارس مكنة الرقابة والاشراف عليها ، ونلاحظ مدى التناقض بين الموقفين مما لايسمح بوجود كلا الفكرتين معا .

وعرف الفقه شركات الاستثمار المالية بكونها (نوع من انواع الشركات التي يكون نشاطها استثمار الاموال لحساب الغير بادارة الاوراق المالية والتعامل بها) [6]، ومما يلاحظ على التعريف اعلاه انه ضيق من مفهوم شركات الاستثمار المالي فقد ركز بشكل كبير على الجانب العام لنشاط الشركة ولم يبين الجانب الموضوعي بشيئ من التفصيل ولم يحدد الية الاستثمار وكيفية التعامل بالاوراق المالية .

في حين ذهب جانب اخر من الفقه الى تعريف شركات الاستثمار المالي بانها (شركات مساهمة تستثمر اموالها عن طريق شراء الاسهم السندات التي تعود لشركات اخرى وبيعها لتحقيق الارباح وتوزيعها على المساهمين وتكون مسؤولة عن اختيار الشركات التي تستثمر فيها ليكون المساهمون اكثر اطمئنانا على

---

[1] د. هيام الجرد ، المد والجزر بين السرية المصرفية وتبييض الاموال ، ط1 ، منشورات الحلبي الحقوقية ، لبنان، بيروت، 2004 ،17 .

[2] انظر نص المادة (1) منن قانون المصارف العراقي رقم 94 لسنة 2004 .

[3] د. عبد المنعم السيد علي ، النقود والمصارف والاسواق المالية ، دار الحامد للنشر ، ط1 ، 2004، ص 137 .

[4] انظر نص المادة (9/اولا) من قانون الشركات العراقي رقم (21) لسنة 1997 المعدل .

[5] انظر نص المادة (9/ثانيا) من قانون الشركات العراقي رقم 21 لسنة 1997 المعدل .

[6] د. لطيف جبر كوماني ، الوجيز في شرح قانون الشركات الاردني ، دار الابجدية للنشر والتوزيع ، عمان ، 1994 ، ص176.

اموالهم وعلى مصـــيرهم مبتعدة عن عمليات التمويل والســـيطرة او المضـــاربة التي قد تكون في بعض الاحيان اثارها اكثر ضررا على هؤلاء المساهمين)[1].

وبناء على ما تقدم فان لشـركات الاسـتثمار المالي شـخصـية قانونية مسـتقلة وذمة مالية تمتلك من خلالها موجوداتها ، وتلتزم الشـــركـة كمـا هو معروف بعقدهـا الـذي وجدت من خلاله والذي يســـتلزمه القانون لممارسة اعمالها ، ويحدد اوجه نشاطها لتتقيد بها وان يكون هدفها الوحيد هو ادارة محفظة الاوراق المالية للحفاظ على اموال المساهمين (المستثمرين) وادارتها بما يحقق مصالحهم.

من خلال كل ما ذكر نستطيع ان نقول بان الشركات المالية في المجمل تكون على نوعين ، شركات مالية مصـرفية تقوم بالعمل المصـرفي كالمصـارف ، وشـركات مالية غير مصـرفية لا تقوم بالعمل المصـرفي وانما لها مجالها الخاص في الاستثمار المالي كما في شركات الاستثمار المالي ، وشركات التحويل المالي .

بيد انه لا يكتمل مفهوم البيانات الشخصية لزبائن الشركات المالية من خلال تعريفها فقط ، بل يجب علاوة على ذلك ان نحدد طبيعتها القانونية وبيان نطاقها وهو ما سنتعرض له في المطلب الاتي .

المطلب الثاني

ذاتية البيانات الشخصية

اقرار المشرع للشخص بحماية بياناته الشخصية ولكن لا يكفي ذلك ان لم تحدد طبيعة هذه البيانات اي بيان السـلطة التي يخولها القانون للشـخص على بياناته وايضـا النطاق الذي رسـمه القانون لهذه البيانات بحيث تكون محمية به ، ومتى تخرج عن اطار حمايته وهو ما سنتناوله في هذا المطلب وكالاتي :

الفرع الاول

ذاتية البينات الشخصية من حيث الطبيعية

شـغلت المسـألة الخاصـة بتحديد الطبيعة القانونية للبيانات الشـخصـية بال الفقه والقضـاء منذ زمن طويل ، حتى قبل ان تتناولها بعض التشـريعات ، ورغم بيان اغلب القوانين المقارنة للبيانات الشـخصـية وتوفير الحمـايـة القـانونيـة لهـا ، الا ان هذه القوانين تفـاوتـت في تطرقهـا لها وبيان طبيعتها القانونية ، ولم يكن هذا الامر قاصـرا على الساحة التشريعية بل وجد مصداقه كذلك في نطاق الفقه القانوني ، لنجد لذلك الاختلاف في تحديد الطبيعة القانونية ســـاحة رحبة في اوســـاطه ، فأتت اراء الفقهاء مختلفة باختلاف الزاوية التي ينظر منها الفقه للطبيعة ومضمون البيانات لان ذلك يختلف بحسب اختلاف الفهم لمعنى البيانات الشخصية اولا ، وفيما اذا كان ينظر لها كحق ملكية ام من قبيل الحقوق اللصيقة بالشخص الطبيعي وهو ما سنتناوله تباعا .

---

[1] د. دياب سـليمان ، اقتصـاديات النقود و البنوك ، المؤسـسـة الجامعية للدراسـات والنشـر والتوزيع ، بدون مكان نشـر، 1996، ص115.

اولا :. حق ملكية : ذهب البعض من الفقه الى ان حق الشخص على بياناته الشخصية هو من قبيل حق الملكية [1] ، ويعد الشخص مالكا لهذا الحق ، فلا يجوز الاعتداء عليه ، فكانت الفكرة السائدة لدى هؤلاء ان للانسان حق ملكية على جسده وشكله جزء من هذا الجسد وثم تطورت لتتناول الحق في البيانات الشخصية وكافة مظاهره ، وترتب على هذا المفهوم نتائج عدة اهمها ، انه من حق الشخص مواجهة الاعتداء على حقه دون حاجة الى اثبات ضرر نتيجة هذا الاعتداء ، كما يجوز للشخص التصرف في جسده ، اذ ان القانون اعطى الشخص الحق في استعمال او استغلال او التصرف في ملكيته ، ومثال ذلك يحق للشخص ان يبيع صورته او شكله ، ومن ثم لا يجوز تصوير الشخص واستغلال صوته دون رضاه او تخزين بياناته والتصرف فيها دون موافقته [2].

وبناء عليه كان اقرب الوسائل الى تكييف الحق في البيانات الشخصية بهذا الاتجاه هو اعتباره حق ملكية على اساس انه اكثر الحقوق انتشارا ورسوخا في الفكر القانوني ويستطرد اصحاب هذا التوجه في انه كما يحق للشخص ان يتصرف في ملكه يجوز له التصرف في بياناته متى كانت قابلة للتداول [3].

ومن كل ما سبق يتبين ان اصحاب هذا الاتجاه يرون في حق الملكية المصداق الامثل الذي يخول الشخص سلطة مطلقة في استغلال واستعمال والتصرف في بياناته الشخصية ، ويمتد هذا بتصورهم الى الحق في حماية البيانات الشخصية ، علاوة على ان الاعتداء على هذه البيانات يخول صاحبها طرق باب القضاء دون الحاجة الى اثبات تضرره ، استنادا الى حق المالك على ملكه [4]. وعلى الرغم من وجاهة الحجج التي استند عليها اصحاب هذا الاتجاه في التأصيل للحق في حماية البيانات الشخصية الا انها لم تسلم من الانتقادات التي وجهت اليها ، فرأي فقهاء هذا التوجه لم يلق استحسانا وقبولا من جانب البعض من الفقهاء والباحثين ووجهوا له نقد من عدة جوانب ابرزها :.

1- ان خصائص حق الملكية تتعارض مع خصائص الحق في حماية البيانات الشخصية ، فاذا كان الحق في حماية البيانات الشخصية يحتج به في مواجهة الكافة شأنه شأن حق الملكية الا ان الاختلاف وحسب رأي هؤلاء يكون في طبيعة هذا الحق ، فالحق في الملكية يفترض وجود صاحب الحق ومحل للحق يمارس عليه ، ففي الحق العيني هو ان يمارس المالك سلطاته على محل الحق فاذا اتحد محل الحق مع صاحبه فيستحيل ممارسة هذه السلطات على الحق وهذا ما ينطبق على الحق في البيانات الشخصية فلا يمكن ان يكون للشخص على ذاته حق ملكية على حسب تعبيرهم [5].
2- ان القول بان الحق في البيانات الشخصية هو حق ملكية وصف ليس دقيق لانه لا يضمن الحماية اللازمة حسب رأي المعارضين لتصوير الحق في البيانات الشخصية كحق ملكية ، ومما يؤكد انتقادهم ان الانسان لا يستطيع حرمان غيره من تصويره ، سيما بعد انتشار آلات التصوير في الشوارع والمحلات وحتى في المساكن اضافة الى ان مالك المنزل يصعب عليه منع المارة من تصوير عقاره من الخارج [6].

---

[1] د. اسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دار النهضة العربية ، القاهرة ، 1994 ، ص29.

[2] د. معاذ سليمان الملا ، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الالكترونية الحديثة ، بحث منشور في مجلة الحقوق كلية القانون جامعة الكويت ، العدد الثالث ، 2018 ، ص 122 .

[3] د. حسام الدين كامل الاهواني ، الحق في احترام الحياة الخاصة ، دار النهضة العربية ، القاهرة ، 1978 ، ص 142.

[4] د. د حسام الدين كامل الاهواني ، مصدر سابق ، ص 143 .

[5] د. خالد ممدوح ابراهيم ، الجريمة الالكترونية ،ط1 ، الدار الجامعية ، الإسكندرية ، 2008 . ص 35 .

[6] د . محمد الشهاوي ، الحماية الجنائية لحرمة الحياة الخاصة ، دار النهضة العربية ، القاهرة ، 2005 ، ص 140.

3- واخيرا من الانتقادات التي وجهت الى اصـــحاب نظرية الملكية انهم ذهبوا الى ادراج الحق في البيانات الشـخصـية تحت حق الملكية حتى لا يخلق حقوقا جديدة ، وكان الاولى بهم بحسـب كلام المنتقدين تحليل هذا الحق تحليلا منطقيا من اجل خلق تفرعات قانونية جديدة يمكن بواســطتها توفير الحماية القانونية له ، وتأثرهم في ارجاع كل جديد الى تقســيمات الحقوق التي اســتمدها المشرع الفرنسي من القانون الروماني الذي وضعهم في تناقض سيما وان قضاة الرومان اكدوا على انه ليس للشـخص حق ملكية على جسـمه [1].وبناء على هذه الانتقادات توجه اصـحابها الى التأصيل للحق في حماية البيانات الشخصية على انه من الحقوق الشخصية وكالاتي :

ثانيا : حق شخصي :. يذهب هذا الرأي الى ان البيانات الشخصية من الحقوق اللصيقة بالشخص ، اذ انه وبحسب الانتقادات الموجهة الى الرأي الاول القائل بان البيانات الشخصية لصاحبها حق ملكية عليها ، فقد ذهب هذ الرأي الى ان الحق في البيانات الشـخصـية يعد حقا من الحقوق الشـخصـية اللصـيقة بالانسـان والملازمة له [2]، وقد اقر هذا الاتجاه المشرع الفرنسي في المادة (9) من القانون المدني وكذلك المشرع المصري في القانون المدني اذ نص على ان " لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته ان يطلب وقف هذا الاعتداء مع التعويض عما يكون لحقه من ضرر "[3]بينما المشرع العراقي في القانون المدني لم يتطرق الى حماية البيانات الشخصية الا انه اشار في المادتين (40-41) منه الى بعض عناصـر البيانات الشـخصـية كالاسـم واللقب وحمايتهما من اي اعتداء ، وقد بنى اصـحاب هذا الاتجاه على هذا الموقف القانوني نتائج كثيرة ابرزها ان الحق في حماية البيانات الشـخصـية من الحقوق الشخصية اذ يمنح صاحب الحق اللجوء الى المحاكم لوقف الاعتداء او منعه دون انتظار حدوث ضرر ، ودون اثبات صـــدور خطأ من المعتدي والعلاقة الســببية بينهما ، وكذلك يفرض على الكافة التزاما عاما وهو احترام هذا الحق ومقوماته المادية كالحق في ســلامة الجســم ومقوماته المعنوية كحق الشــخص في السمعة والشرف والمعتقد [4].

وحسب هذا الرأي فان الكيان الشخصي للشخص يترسخ في عنصرين احدهما طبيعي والاخر قانوني ، فالعنصر الاول وهو الطبيعي يكون في الشخص نفسه من الناحية العقلية والنفسية والمعنوية ، اما العنصر القانوني فيكون في الحقوق اللصيقة بشخصيته والثابتة بحكم القانون ، كالحق في الصورة والاسم ، والحق في الشرف والاعتبار والكرامة ، والحق في البيانات الشخصية كون ان الكيان الشخصي للانسان يضم جوهر اسرار البيانات الشـخصـية ، لذا فهو يتمتع بالحماية ولا يجوز الاعتداء على مستودع اسراره .[5] ويذهب هؤلاء الى ان الاعتراف بالحق في حماية البيانات الشخصية من الحقوق الشخصية ، ويرتب هذا الاتجاه على رأيهم مجموعة من النتائج التي يمكن اجمالها بالاتي :.

1- ان صـاحب الحق الشـخصـي يسـتطيع ان يتجه الى القضـاء حين الاعتداء على الحق ليطلب اتخاذ الاجراءات المناسـبة لوقفه او منعه ، ولا يلزم باثبات عنصـري الخطأ والضـرر ، ومن ثم تكون الحمـاية اكثر فـاعلية وقوة ممـا لو تركت للقواعد العامة في المســؤولية المدنية التي لا تحقق الا الحماية اللاحقة ، اي بعد الاعتداء على الحق وتولد الضـرر والتعويض لا يفلح او ينفع من الناحية

---

[1] د . حسام الدين كامل الاهواني ، مصدر سابق ، ص 145 .

[2] د . ممدوح خليل بحر ، حماية الحياة الخاصة في القانون الجنائي ، دار النهضة العربية ، القاهرة ، 1983 ، ص 273 .

[3] انظر نص المادة (50) من القانون المدني المصري رقم (131) لسنة 1948 .

[4] احمد هادي كعود ، الحق في الخصـوصـية والجرائم الواقعة عليها ، بحث مقدم الى المعهد القضـائي العراقي ، 2013 ، ص19.

[5] د . احمد فتحي سرور ، الحق في الحياة الخاصـة ، بحث منشـور في مجلة القانون والاقتصـاد ، مطبعة جامعة القاهرة ، العدد 54 ، 1986 ، ص45 .

العملية دائما في محو كل الضـــرر ، وبحســـب رأيهم تكون الحماية قوية حينما تكون عن طريق الوقاية من الاعتداء على البيانات الشخصية في مواجهة الجميع ، فيستطيع الانسان ان يطالب بمنع الجميع من الاعتداء على حقه في حماية بياناته الشخصية[1].

2- من سمات الحماية المضفاة على البيانات الشخصية انها موجهة للكافة من حيث خطابها اذ يجب على الجميع احترام هذه البيانات والالتزام بعدم المســـاس بها اطلاقا ، وهذا التزام يســـري في مواجهة الاشخاص كافة سواء كانوا اشخاص طبيعيين او اشخاص معنويين [2] ، او بمفهوم اخر انه يقع على عاتق الاشخاص كافة احترام بيانات الفرد الشخصية وعدم التطفل عليها او معالجتها او نشر ما يتعلق بها الا بموافقته الصريحة .[3]

3- يذهب هؤلاء الى ان الحق في البيانات الشـخصـية لا ينتقل بالميراث ، لان حقوقه الشـخصـية لا تدخل اصـــلا في ذمته المالية بحســـب اعتقادهم [4] ،اما ما يتعلق بأنتقال الحقوق التي ترتبط بهذا الكيان الى الورثة كما هو الحال في (خصوصيات السلف او شرفه) وذلك لتحديد مسألة حمايتها عن طريق الورثة [5] . وبناء على ذلك انه بأمكان اصحاب الحق الشخصي في بيانات المتوفى اذا ثبت الاعتداء عليها مقاضاة صاحب فعل الاعتداء بأعتبارهم متضررين شخصيا من هذا التعدي على هذه البيانات العائدة لمورثهم ، وعندما يقومون بمقاضاة المعتدي فأن ذلك ليس بوصفهم ورثة المتوفى لان هذا يتعارض مع عدم امكانية انتقال حقوق الشخص بالميراث كم مر ذكره عن هؤلاء ، لكن الضرر قد حل بهم بصفته معتدى عليه فان رفع الدعوى من قبل هؤلاء فانها تأخذ مسارها الاصولي باعتبارهم اصحاب حق لا ورثة .[6]

ورغم الحجج التي نادى بها اصحاب هذا الرأي والنتائج التي توصلوا اليها الا ان نظريتهم لم تسلم من النقد اذ قد تم الرد عليها بعدة نقاط وكالاتي :

1- فيما يتعلق بكون القول بان الحق الشخصي يضفي حماية اكبر للبيانات الشخصية كلام مردود ، كون قواعد المسؤولية تطورت كثيرا ولم يعد يشترط ان تكون هناك الاركان التقليدية للمسؤولية (خطأ وضرر وعلاقة سببية) ، اذ اصبحت هناك فكرة المسؤولية الموضوعية وتقوم هذه النظرية على فكرة قانونية تختلف تماما عن الاســـس القانونية المعروفة في المســـؤولية ، اذ تقوم هذه المسؤولية على محلها او موضوعها ، اي على عنصر الضرر فقط ، اذ يتم التعويض حتى وان لم يثبت ارتكاب المسؤول خطأ ، وتقوم هذه المسؤولية على ركنان (الضرر والعلاقة السببية بين الضرر وفعل المسؤول) ، فكل فعل او عمل يسبب ضرر للغير يلزم فاعله بتعويض المضرور منه ، ولا يمكن لمرتكبه نفي هذه المســـؤولية بنفي الخطأ الثابت او المفترض او حتى بالاحتجاج بالسبب الاجنبي [7]، وعليه فأن هذه النظرية حسب قول الفقه تبدأ بالضرر وتنقضي بالتعويض

---

[1] القاضي اياد محسن ضمد ، حماية حق الخصوصية من تأثير الاعلام في العراق ، مكتبة صباح ، بغداد ، 2017، ص 38 .

[2] د . اسامة عبد الله قايد ، مصدر سابق ، ص 31 .

[3] د . حسام الدين كامل الاهواني ، مصدر سابق ، ص 146 .

[4] د . محمد حسين منصور ، نظرية الحق ، دار الجامعة الجديدة ، الاسكندرية ، 1998 ، ص 117 .

[5] د . حسام الدين كامل الاهواني ، مصدر سابق ، ص158 .

[6] د. محمد حسن قاسم ، المدخل لدراسة القانون – القاعدة القانونية ، نظرية الحق ، ج2 ، منشورات الحلبي الحقوقية ، بيروت ، 2009 ، ص101 .

[7] د. محمد سعيد عبد الله الحميدي، المسؤولية المدنية الناشئة عن تلوث البيئة البحرية والطرق القانونية لحمايتها وفقا لقانون دولة الامارات العربية المتحدة ، ط1 ، دار الجامعة الجديدة ، الاسكندرية ، 2008 ، ص 332-333

دون ان تكون هناك رابطة سببية بين نقطة البداية ونقطة النهاية [1].مما يعني ان النتيجة التي توصل اليها هؤلاء في كون الحماية التي توفرها الحقوق اللصيقة بالشخصية نتيجة ممكن ان تكون متحققة اذا اعتبرنا ان الحق في البيانات الشخصية هو في حقيقته حق ملكية ، هذا الحق الذي يمكن صاحبه من ممارسة سلطاته (الاستعمال والاستغلال والتصرف) بخلاف القيود التي تفرضها الحقوق اللصيقة بالشخصية .

2- كذلك يمكن الرد على النتيجة الثانية التي توصل اليها اصحاب وجهة الحق اللصيق بالشخصية في كونها تفرض احترامها على الكافة ، بان ذات النتيجة تتحقق بالنسبة لحق الملكية كذلك ، اذ ان هذا الحق يكون مانعا للكل في ان يتطفلوا عليه او يزاحموا المالك الا بموجب القانون .

3- والاشكالية الاخرى التي اثارها اصحاب رأي الحقوق اللصيقة بالشخصية هي كون البيانات الشخصية لا تنتقل بالميراث وهذه من طبيعة الحقوق اللصيقة بالشخص بخلاف حق الملكية الذي ينتقل الى الخلف العام ، لكن يمكن ان يرد على هذا التصور في كون لا ينسجم مع الاهمية التي تحضى بها البيانات الشخصية في الوقت الحاضر وفي ظل التطور التكنولوجي ، اذ اجازت التشريعات الحديثة انتقال البيانات الشخصية للورثة كما في الولايات المتحدة الامريكية في ولاية (ديلاوير)[2]والتي تعد اول ولاية امريكية وضعت تشريعا ينظم الية انتقال البيانات الشخصية والتي تمكن الوارث من حيازة الحسابات الرقمية والاصول للمورث ومن ثم اتبعتها ولايات اخرى . اضافة الى ذلك فان قانون ديلاوير قد جعل طرق انتقال التركة الرقمية تنطبق على جميع الاصول الرقمية سواء كانت اصول رقمية مالية او شخصية ، فلم يفرق بين الاصول الرقمية الشخصية والاصول الرقمية المالية [3] .

وعند التمعن في نصوص قانون ولاية ديلاوير المذكور ، يتبين ان الفصل (5005 /أ) منه والخاص بالحسابات و بالاصول الرقمية النافذ ، قد اشار الى قاعدة عامة تحكم خلافة المتوفي في حساباته واصوله ، اذ نص على انه (يتمتع المؤتمن (الوارث) بموجب هذا الفصل بسلطة على الاصول الرقمية او الحسابات الرقمية هي نفس سلطة صاحب الحساب على اصوله وحساباته)[4] .

ويلاحظ على النص اعلاه انه قد تبنى قاعدة عامة تتمثل في جعل صلاحيات الوارث او من ينوب عنه هي نفس صلاحيات صاحب التركة الرقمية المتوفى على اصوله وممتلكاته الرقمية .

اما بخصوص موقف القضاء فقد ذهب القضاء الامريكي الى الحث على انتقال البيانات الشخصية من خلال تقريره لمثل هذا الحق ، ففي قضية ورثة (آجمان ضد شركة ياهو) عام 2009 قضت المحكمة

---

[1] د. احمد محمود سعد ، استقراء لقواعد المسؤولية المدنية في منازعات التلوث البيئي، ط1 ، دار النهضة العربية ، القاهرة ، 1994 ، ص 281 .

[2] عند تتبع جذور قانون ولاية ديلاوير نجد ان الولاية اعتمدت على مسودة مشروع القانون الموحد لوصول المؤتمن للاصول والحسابات الرقمية للمتوفى المعروف اختصارا (UFADAA) وهو مشروع قانون اعد عام (2014) من قبل مجموعة من الخبراء ، وقد وافقت عليه لجنة القانون الموحد الامريكي المعنية بمراجعة مشاريع القوانين التي تعرض على مجلس النواب ، الا ان القانون بالرغم من انه عرض على مجلس النواب الا انه لم يصوت عليه الى الان ، بسبب المعارضة الشديدة من قبل الشركات المزودة للخدمات التي طلبت اجراء التعديلات على مسودة القانون.

-Elizabeth Holland Capel 17 Elizabeth Holland Capel , Conflict and Solution in Delawar,s Fiduciary Access to Digital Assets and Digital Accounts Act , Volume 30 , Issue 4 Annual Review the Law Journals and Related Materials at Berkeley Law , 2015 .p. 1212 -1213 .

[3]Elizabeth Holland Capel ,op . cit .P 1220.

[4]5005 "(a) A fiduciary with authority over digital assets or digital accounts of an account holder under this chapter shall have the same access as the account holder ,……"

العليا في ولاية ماساتشوستي الامريكية . في حق الورثة في ان يحلوا محل مورثهم في حساباته ومحتوى هذه الحسابات عند مطالبتهم بذلك شرط ان لا تكون هناك وصية للمتوفى ، وقضت المحكمة بالزام الشركة من تمكين المدعيين من الوصول الى البريد الالكتروني للمورث [1].

وفي ذات السياق ذهب القضاء الالماني اذ قضت محكمة العدل الاتحادية الالمانية (ان وسائط المستخدم الاجتماعية الرقمية و حساباته قابلة للتوريث عند موت صاحب الحساب ، ويطبق قانون الميراث على توزيع حقوق المورث حسب نص المادة (1922 من القانون المدني) ولا يجوز الاتفاق على منع الورثة من حق الوصول الى محتوى حسابات مورثهم)[2].

ومن خلال ذلك يتبنى الباحث الرأي القائل بكون الحق في البيانات الشخصية هو من قبيل الملكية لقوة ورجاحة الحجج التي استدل بها انصاره ، فمن جانب لم يعد هناك شك حول القيمة الاقتصادية للبيانات والمعلومات الشخصية ، وامكانية تقويمها بسعر السوق كما سنبينه لاحقا ، الامر الذي يوضحه انتشار شركات تجميع المعلومات والبيانات الشخصية والتعامل بها ، وتزايد السباق نحو الحصول على بيانات الاشخاص ومعلوماتهم الشخصية بطرق الكترونية متعددة ومستحدثة كما سيأتي بيانه لاحقا ، ومن جانب اخر علاقة التبعية التي تربط بين البيانات الشخصية وصاحبها ، هي ذاتها العلاقة التي تربط المالك

---

[1] تتلخص وقائع الدعوى (توفي سنة 2009 شخص يدعى جون آجمان في حادث ، وقد ترك وراءه حساب على موقع ياهو ، ولم يترك وصية او توجيه لتحديد مآل الحساب ، بعد ذلك عينت المحكمة الوصاية والاسرة اشقاء جون ، روبرت ومارين ، كخافاء لممتلكات شقيقهما ، اتصل احد الاشقاء في شركة ياهو للحصول على البريد الالكتروني لمورثهم الا ان شركة ياهو رفضت ذلك ، رفعت شقيقة المتوفى سنة 2009 دعوى ضد الشركة تطالب بالوصول الى البريد الالكتروني لشقيقها المتوفي ، في البداية رفضت محكمة الموضوع طلب الاشقاء في الوصول الى بريد مورثهم بداعي ان قانون الاتصالات الاتحادي الامريكي يمنع ذلك ، لكن اصرت مارين وبعد ذلك تم الطعن بالحكم امام المحكمة العليا التي نقضت قرار المحكمة الابتدائية ، والزمت الشركة بتمكين الخلف العام من الوصول الى ممتلكات مورثهم ، واستندت على حجة عدم وجود ما يعارض في قانون الاتصالات الامريكي او اي قانون من انتقال الحسابات والاصول الشخصية للورثة) Case Law \- Ajemian v. Yahoo !,Id no : 778 , 74 – 773 ...

[2] ففي قضية تتلخص وقائعها :(ان شابة قد توفت في عمر 15 عام بحادث قطار ، وادعى والديها ضد شركة فيس بوك في يناير 2017 انهم حاولوا الوصول الى حساب ابنتهم المتوفية وكلمة المرور لتسجيل الدخول للحساب الا ان الشركة لم تستجب لطلبهم ، وقد حولت شركة فيس بوك ملف تعريف ابنتهم (الصفحة) الى ما يسمى صفحة تذكارية وهي خدمة تمنع الوصول الى بيانات المستخدم نهائيا ولم يمكن تسجيل الدخول اليها ، لكن يبقى المحتوى من منشورات وصور وذكريات على الصفحة ويبقى مرئيا للجمهور من الاصدقاء . وبعد ذلك حكمت المحكمة الابتدائية لصالح الوالدين بالحصول على حساب ابنتهم ، لكن نقضت محكمة الاستئناف حكم المحكمة الابتدائية ، بحجة ان سرية الاتصالات منعت المدعى عليه من نقل محتوى الاتصالات الى الورثة وهو منع صحيح ، الا ان محكمة العدل الاتحادية ، نقضت قرار محكمة الاستئناف في سنة (2019) وحكمت لصالح المدعى عليه (الوالدين) بمنحهم حق الوصول للحساب ومحتواه ، وسببت حكمها بحجج متعددة اهمها : ان العقد المبرم بين المستخدمة المتوفاة وشركة فيس بوك يجب ان تنتقل اثاره الى الخلف العام بموجب القانون وفقا للمادة 1922 من القانون المدني الالماني ، ولايمكن للشروط التعاقدية في هذا العقد ان تستبعد قواعد الارث ، كما وخلصت المحكمة الاتحادية الى خدمة الصفحات التذكارية ليست جزءا من الشروط والاحكام العامة في العقد المبرم علاوة على ذلك رأت المحكمة انه حتى لو كانوا جزءا من الشروط والاحكام العامة ، فانها لن تكون صالحة للتنفيذ ، لانها تضر بشكل غير معقول بالطرف الاخر فيالعقد ، كما وانها تحظر بصورة غير مباشرة تطبيق قواعد الارث ، وتقوضها بمنع وصول الورثة الى الحساب ، كما ذكرت المحكمة العليا ان قرار محكمة الاستئناف يمنع الورثة من ممارسة حقوقهم باتلاف البيانات والتخلص منها وهي من الحقوق الاساسية التي نشأت للمستخدم المتعاقد ومن ثم الى الورثة من بعده).

Case KG Berlin Vorinstanzen:no(31.05.2017-21u9\16)date(Jul2018).

الموقع الرسمي لمحكمة العدل الالمانية

http :\\www.loc.gov\law\foreign-news\article\germany-federal-court-of-jusice-rules-digital-social-media-accounts-inheritable.

بالشيء المملوك ، الامر الذي يعطي لصاحب البيانات والمعلومات الشخصية الحق في ضمان سرية بياناته ومعلوماته ، فضلا عن حقه في الحصول على التعويض عن اي اعتداء عليها .

الفرع الثاني

ذاتية البيانات الشخصية من حيث النطاق

يعد موضوع تحديد نطاق البيانات الشخصية من الاهمية بمكان اذ يحضا بتنظيم يجد مساحته في التشريعات المقارنة التي صدرت بهذا الشأن ، نظرا لما يترتب على ذلك من معرفة البيانات التي تحمى بموجب هذه القوانين ، والاشخاص محل الحماية القانونية وهو ما سنتناوله تباعا في الفقرات الاتية :

اولا : النطاق الموضوعي للبيانات الشخصية :. اشارت اللائحة الاوربية على ان يعمل باحكام هذه اللائحة وتطبق احكامها على معالجة البيانات كليا او جزئيا بوسائل آلية وعلى المعالجة بخلاف الوسائل الالية للبيانات الشخصية التي تشكل جزءا من نظام حفظ الملفات او يقصد بها ان تشكل جزءا من نظام حفظ الملفات [1].

في حين اشار المشرع المصري الى انه يعمل باحكام هذا القانون والقانون المرافق في شأن حماية البيانات الشخصية المعالجة الكترونيا جزئيا او كليا عند اي متحكم او حائز او معالج لها ، وذلك بالنسبة للاشخاص الطبيعيين [2]، اذ نلاحظ بأن تطبيق هذا القانون يقتصر نطاقه على البيانات المعالجة الكترونيا فقط [3]، ولا يمتد الى معالجة البيانات المخزونة ورقيا بصورة كاملة او المكتوبة اذ يتمثل تطبيق القانون للبيانات المعالجة الكترونيا بصورة جزئية ، وهو تقييد ينصرف بطبيعة الحال الى البيانات المخزونة ورقيا ثم تجري معالجتها بطريقة الكترونية ، ولا تختلف البيانات الشخصية التقليدية عن البيانات الشخصية الرقمية الا في ان الاخيرة تستخدم عند التعامل بالوسائط الالكترونية .فكلتاهما عبارة عن البيانات الشخصية لكل

---

[1] انظر المادة (1/2) من اللائحة الاوربية لحماية البيانات الشخصية .

[2] انظر المادة الاولى من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 ، علما ان المشرع المصري قد بين معنى المصطلحات الواردة في أعلاه في المادة (1) من قانون حماية البيانات الشخصية النافذ وهي الاتي (الحائز هو شخص طبيعي او اعتباري يحوز ويحتفظ قانونيا او فعليا بيانات شخصية في أي صورة من الصور ، او على اية وسيلة تخزين سواء اكان هو المنشئ للبيانات ، او انتقلت اليه حيازتها باية صورة) في حين عرف المتحكم بانه (أي شخص طبيعي او اعتباري ، يكون له بحكم او طبيعة عمله – الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها طبقا للغرض المحدد او نشاطه) . بينما عرف المعالج بانه (أي شخص طبيعي او اعتباري مختص بطبيعة عمله بمعالجة البيانات الشخصية لصالحه ، او لصالح المتحكم بالاتفاق معه ووفقا لتعليماته) .

[3] عرفت المعالجة الالية بانها (كل عملية تتم بالوسائل الالية وتتعلق بجمع البيانات او تسجيلها ، او القيام بالتعديلات او الاحتفاظ او تدمير المعلومات او البيانات الاسمية او أي عملية من ذات الطبيعة تتصل باستغلال الملفات او قواعد البيانات خصوصا الاطلاع عليها او تبادل البيانات الاسمية او حفظ واتلاف بيانات اسمية ، كذلك كل عمليات من ذات الطبيعة تتصل باستغلال او استثمار الملفات او قواعد البيانات و بالذات تقنيات التواصل والتقارب عبر شبكة الانترنت ، الاطلاع او نقل وبث البيانات الشخصية). ينظر الدكتور خالد حسن احمد ، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية ،ط1 ، دار الكتب والدراسات العربية ، القاهرة ، 2020 ، ص56 .

انســان والتي تشــمل الاســم ولقب الشــخص ورقم هاتفه والرقم البريدي والســن والجنس وتاريخ الميلاد والجنســية وغيرها من البيانات التي يمكن من خلالها تحديد صــاحبها او يكون قابلا للتحديد ، ولاينكر ان البيانات الشخصية للافراد حق من حقوقهم الاساسية والتي تجب حمايتها مدنيا وجنائيا . [1]

ويرى الباحث ان لكل انسان الحق في حماية بياناته الشخصية عند اتصاله بطريقة الكترونية ، وهذا الحق ينطبق كذلك على كل معالجة للبيانات الشخصية تقوم بها الشركات المعنية ، ومن ثم يكفل القانون الحماية القانونية للبيانات الشــخصــية في العالمين التقليدي والرقمي . نظرا لوحدة الوظائف والاهداف وان اختلف اســلوبها من الجهة التقنية ، فلا عبرة للطريقة التي تتم بها معالجة البيانات الواردة او المتوقع ورودها في ملفات ورقية او طريقة الكترونية او حتى صــورة وســواء تمت المعالجة بطريقة آلية او غير آلية كليا او جزئيا وكلتا الطريقتين تمتد اليهما الحماية القانونية ، وندعو المشــرع العراقي بدورنا الى الاخذ بوجهة النظر هذه في حال اقراره لقانون يحمي البيانات الشــخصــية مستقبلا .وعددت التشــريعات محل المقارنة البيانات الشــخصــية وان كانت هذه البيانات لم تذكر في القوانين على سبيل الحصــر ، لانها مسألة نسبية ومختلفة من زمن لاخر ولربما تظهر بيانات اخرى مستقبلا تدخل في نطاق البيانات الشخصية ، او يكون احد البيانات حاليا لكنه لايكون كذلك مستقبلا .

لكن الفقه بدوره حاول بيان هذه البيانات الشــخصــية وان كان قد اختلف في ذلك ، فهناك من ذهب الى ان اسم الشخص المقترن برقم هاتفه والمعلومات المتعلقة بظروف عمله او هواياته تعد بيانات شخصية [2]، في حين ذهب بعضــهم الى انه يعد بيانا شخصيا اسم العائلة والاسم المعطى لبعض الاشخاص الطبيعيين الذين يتجاوز دخلهم حدودا معينة بالاضافة الى مقدار الدخل المكتسب وغير المكتسب [3]. وذهب اخرون الى انه تشكل البيانات المتعلقة بالزبون او المشترك حين تقديم الطلب للحصــول على الخدمات المختصــة بها الشركة مثل (الاسم وتاريخ الميلاد او الجنسية او الجنس ، والعرق ، والدين ، واللغة) بيانات شخصية في حين قصرها بعضهم على صورة الشخص المسجلة بواسطة الكاميرا لانها تجعل من الممكن التعرف على الشــخص المعني [4] .في حين رأى جانب اخر من الفقه على ان البيانات الشــخصــية اضــافة لما ذكر فانها تشمل البيانات الضريبية ودخل الفرد ومقدار ثروته ، وان توصيف المعلومات المتعلقة بشخص ما على انها بيانات شخصية لا يعتمد على ما اذا كان الشخص يعترض على الكشف عن تلك المعلومات ام لا ‘ وانما هل ان هذه البيانات كافية للكشــف عن احواله الشــخصــية والمادية فاذا كانت كذلك فهي اذن بيانات شــخصــية [5]، وما دام المشــرع المصــري وكذلك اللائحة لم يحدد هذه البيانات فاننا نعتقد بصــحة الرأي الاخير في تحديد هذا النطاق مادامت المعلومات لم تكن مباحة قانونا ، اذ تم اســتثناء معلومات معينة من

---

[1] د. طارق جمعة السيد ، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، بحث منشور في مجلة القانون والاقتصاد المصرية ، ملحق العدد 94 ، 2021 ، ص5 -6 .

[2]Nadezhda Puytova , Tocite this article ; Nadezhda(2018) The law of every thing . Broad concept of personal data and Future of E U data Protection law ,Innovation and Technology , 10:1 , 40 -81,dol: 10-1080\17579961, 2018 ,p145.

[3] د. شريف يوسف خاطر ، حماية الحق في الخصوصية المعلوماتية ، بحث منشور في مجلة البحوث القانونية والاقتصادية ، جامعة المنصورة ، العدد 57 ، 2015 ، ص39 .

[4] د. عبد الرحمن خليفة الرواس ، اثر التشريعات المتعلقة بحماية البيانات الشخصية على فعالية التجارة الالكترونية ، ط1، منشورات زين الحقوقية ، لبنان، 2019 ، ص114 .

[5] د. جبالي ابو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية ، بحث مقدم الى مؤتمر العصر الرقمي واشكالياته القانونية ، كلية الحقوق ، جامعة اسيوط ، من 12-13 ابريل 2016 ، ص4.

الشمول بالحماية ، اذ اشار المشرعان المصري والاوربي الى طائفة من البيانات الشخصية [1] ، وان كانت تعد شخصية اي خاصة بالا شخاص الطبيعيين ، ومعالجة الكترونيا كليا او جزئيا ولكن لا تسري عليها احكام قانون حماية البيانات الشخصية ، ولا تتمتع بالحماية ، وذلك بغية تحقيق اهداف ومرابي متنوعة ، فتقتصر الحماية على البيانات الشخصية التي تتم في اطار تجاري او مهني ، وتخرج من نطاقها البيانات التي تتم معالجتها في اطار او سياق شخصي بحت [2]، وهو استبعاد يتماشى مع المنطق ، اذ ان الهدف من التنظيم القانوني لحماية البيانات الشخصية هو منع تعرضها للانتهاك او الاستغلال من جانب الغير ، اما هنا فمن غير المتصور ان يكون الاستعمال الشخصي محلا لانتهاك الخصوصية والاستغلال ، وكذلك تخرج من اطار البيانات الشخصية اذا كان الاستغلال لاغراض اعلامية بشرط ان تكون صحيحة ودقيقة ، والا تستخدم في اغراض اخرى ، وذلك دون الاخلال بالتشريعات المنظمة للصحافة والاعلام [3].

وكذلك يمكن الاطلاع على البيانات الشخصية اذا ما كانت مرتبطة بالحفاظ على الامن القومي ، واغراض منع الجرائم او ضبط مرتكبيها او تنفيذ العقوبات واعمال السلطة القضائية[4] ، ويجب على الشركة هنا وبناء على طلب من الجهات الامنية اخطار المتحكم او المعالج بتعديل او محو او عدم اظهار او اتاحة او تداول البيانات خلال مدة زمنية محددة ، وفقا لاعتبارات الامن ، ويلزم المعالج او المتحكم بتنفيذ ما ورد بالاخطار خلال المدة الزمنية المحددة به [5] ، وايضا ذهب المشرع المصري الى استثناء البيانات الشخصية لدى البنك المركزي المصري والجهات الخاضعة لرقابته واشرافه ، عدا شركات التحويل المالي وشركات الصرافة على ان يراعى في شأنها القواعد المقررة من البنك المركزي بشأن التعامل مع البيانات الشخصية ، الا انه هناك من ذهب الى رفض هذا الاستثناء بالنسبة للبنك المركزي والجهات التابعة له ، كونه يفرغ القانون من محتواه ويجعله بلا قيمة ويمثل عدم استيعاب لفلسفة حماية البيانات الشخصية والتي تعد حقا اصيلا للانسان [6].

ومن خلال ذلك نلحظ ان المشرع المصري قد ذهب في قانونه الجديد المشار اليه في أعلاه الى استبعاد طائفة كبيرة من البيانات الشخصية من نطاق الحماية رغم حاجتها كما يرى الباحث لاضفاء الحماية عليها ، ودون مبرر او علة معتدا بها ، ومن ذلك البيانات الشخصية لدى البنك المركزي ، والبيانات المتعلقة بمخاطر الضبط القضائي والتحقيقات والدعاوى القضائية وكذلك لدى الجهات الامنية ، حيث كان من الاولى وضعها تحت مظلة الحماية وفق ضوابط تراعي خصوصيتها وليس استبعادها على اطلاقها [7].

ثانيا : النطاق الشخصي للبيانات الشخصية :. ينحصر نطاق تطبيق الحماية القانونية للبيانات الشخصية في التشريعات المختصة على بيانات الاشخاص الطبيعيين ، مما يعني استبعاد الشخص المعنوي العام او

---

[1] انظر نص المادة (1) من قانون حماية البيانات الشخصية المصري والمادة (4) من اللائحة العامة الاوربية لحماية البانات الشخصية رقم 679 لسنة 2016 .

[2] د. عبد الرحمن خليفة الرواس ، مصدر سابق ، ص118 .

[3] د. محمد احمد المعداوي ، مصدر سابق، ص1948.

[4] انظر نص المادة (2/د) من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016.

[5] د. عثمان بكر عثمان ، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي ، اطروحة دكتوراه ، كلية الحقوق جامعة طنطا ، 2020 ، ص31 .

[6] جوهر زايد جوهر المهندي ، الحماية الجنائية لحرمة الحياة الخاصة في القانون القطري " دراسة مقارنة " اطروحة دكتوراه مقدمة الى كلية الحقوق جامعة القاهرة ، 2019، ص49.

[7] د . جوهر زايد جوهر ، المصدر نفسه ، ص53 .

الخاص [1]، وهو منطق محل نظر لا يوجد له تبرير منطقي ، اذ من الثابت ان للشخص المعنوي شخصية قانونية وهو يتمتع بجميع الحقوق الا ماكان منها ملازما لشخصية الانسان الطبيعي [2] ، وايضا باتت بيانات الاشخاص المعنوية تحظى باهمية بالغة في الوقت الحاضر قد تفوق اهمية بيانات الشخص الطبيعي ، وهو ما يحتاج لافراد حماية خاصة لها .اذ من غير المقبول استثناء الاشخاص المعنوية من حماية البيانات الشخصية ، لان المساس بهذه البيانات يمس الحقوق المالية للشخص ، فقد يؤدي ذلك الى المساس بسمعة الشخص المعنوي .

واخذت بعض التشريعات في هذا الاتجاه ومنها قوانين بعض الدول الاوربية كون المقارنة معها، كالقانون الفيدرالي السويسري حول حماية البيانات الشخصية الصادر عام 1992 في المادة (2) منه ان نطاق تطبيق القانون يشمل معالجة البيانات التي تخص الاشخاص الطبيعيين والاشخاص المعنويين .

وان كان من المسلم به ان الشخصية الطبيعية للانسان تبدأ بتمام ولادته حيا ، فيجب ان تكون ولادته تامة ، وان يكون قد ولد حيا ، وتنتهي الشخصية بالموت [3] ، وما بين الولادة والموت يكون الشخص الطبيعي ويتمتع باهلية الوجوب وهي صلاحياته لان تكون له حقوق وعليه والتزامات [4]،فضلا عن اهلية الاداء ومناطها الادراك والتمييز[5] . وبالتالي فأن صاحب البيانات هو كل شخص طبيعي تكون معطياته الشخصية موضوعا للمعالجة ؛ فعلى سبيل المثال البيانات أو المعلومات المدرجة فى الملف الشخصي للموظف بقسم شؤون الموظفين ؛ فهذه البيانات تعبر بصورة واضحة عن المعنى بالأمر من حيث حالته الشخصية بصفته موظفا ، كما ينطبق ايضا على النتائج الخاصة بالفحص الطبي للمريض فى ملفه الطبي الموجود بالمستشفى أو صورة أو فيديو لشخص أثناء إجراء مقابلة معه.

ويشترط أن تكون المعلومات متعلقة بشخص طبيعي محدد أو قابل للتحديد ؛ حيث يرتكز هذا الامر على الاعتبارات الآتية:

بصفة عامة ، يمكن اعتبار الشخص الطبيعي" محدد عندما يكون" متميزًا "من بين جميع الأشخاص الآخرين داخل مجموعة من الأشخاص ؛ بينما الشخص الطبيعي "القابل للتحديد " والذى لم يكن فى الإمكان تحديده بعد. ومن المتفق عليه ؛ أنه يمكن تحديد الهوية عادة عن طريق معلومات خاصة محددة لها علاقة بالشخص المعنى بالأمر ؛ نذكر منها على سبيل المثال ؛ بعض العلامات أو المظاهر الخارجية للشخص مثل طوله ، ولونه ، وشعره ، وملابسه.... إلخ . أو صفه من صفات الشخص التي لا تكون ظاهرة للعامة مثل المهنة والوظيفة والاسم.

ولكن السؤال الذي يرد هنا هو هل يكتفي بكون الشخص صاحب البيانات شخصا طبيعيا فقط حتى تكون بياناته الشخصية محل حماية ام يجب ان يكون في مكان معين او الشركة التي تقوم بالمعالجة في بلد القانون ؟

---

[1] د. طارق جمعة السيد راشد ، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، بحث منشور في مجلة القانون والاقتصاد ، ملحق العدد 94 ، 2021 ، ص 31.

[2] انظر نص المادة (2/48) من القانون المدني العراقي رقم (40) لسنة 1951 ، وكذلك نص المادة (1/53) من القانون المدني المصري رقم 131 لسنة 1948 .

[3] انظر نص المادة (1/34) من القانون المدني العراقي وكذلك المادة (29) من القانون المدني المصري .

[4] د. حسن علي الذنون ، النظرية العامة للالتزامات (مصادر واحكام الالتزام) المكتبة القانونية ، بغداد ، 1976 ، ص78 .

[5] د. حسن علي الذنون ، المصدر نفسه ، ص80 .

حقيقة الامر ذهبت اللائحة الاوربية لحماية البيانات الشخصية في تحديد النطاق الاقليمي لتطبيق احكامها ، اي الاخذ بمعيار موطن المعالج او المتحكم في البيانات بصرف النظر عما اذا كانت المعالجة تتم في دول الاتحاد الاوربي ام لا ، كما تنطبق اللائحة على البيانات المتداولة داخل الاتحاد رغم وجود المعالج او المتحكم خارج الاتحاد متى تعلقت انشطة المعالج بعرض سلع او خدمات لاصحاب هذه البيانات داخل الاتحاد الاوربي ، او يوجد في مكان يطبق فيه قانون الدول الاعضاء [1]، اما في مصر فأن المشرع المصري اخذ بمعيار الجنسية المصرية للشخص المعني بالبيانات او محل اقامته في مصر ، بصرف النظر عن مكان وقوع الفعل الخاطئ وايا كان محل تواجد المخطئ [2]، وقد تثور هناك مشكلة تنازع القوانين وخاصة في حالة الاعتداء على بيانات المواطن المصري من الخارج ، وايضا اشترط المشرع المصري ان يكون الفعل معاقبا عليه في الدولة التي وضع فيها ، وهو مايزيد الامر تعقيدا في مجال تنازع القوانين مما يؤدي بطبيعة الحال الى عدم امكانية تطبيقه في هذه الحالة .

ومن خلال ما تقدم من عرض للنطاق الموضوعي والشخصي للبيانات الشخصية نستطيع ان نشير الى بعض من اهم صور البيانات الشخصية وان كان تحديدها بطريقة مسبقة ليس امرا يسيرا لانه من المتصور ان تظهر في المستقبل صور لهذه البيانات الشخصية .

وما يرغب الباحث في التأكيد عليه هنا هو ان ما يتم طرحه من صور البيانات الشخصية ليس على سبيل الحصر وانما على سبيل المثل والدلالة ، وهذه الصور هي التي جرى العمل على اعتبارها بيانات شخصية تحمى بموجب القانون الى وقتنا الحالي . مما يعني من الممكن ظهور صور اخرى لهذه البيانات في المستقبل تكون خاضعة للحماية القانونية حسب التطور التقني والتكنولوجي المستقبلي ولهذا نستطيع ان نذكر اهم هذه البيانات وعلى النحو الاتي :

1- البيانات الشخصية الاجتماعية :. تعد هذه البيانات اساس دراسة البيانات الشخصية وتتمثل في عدة صور مثل [3]:

أ – الاسم واللقب : الاسم هو وسيلة لتفريد الشخص وتمييزه عن غيره ، وقد يستخدم الاسم بالمعنى الضيق للدلالة على اسم صاحبه وحده ، او بالمعنى الواسع لبيان اسم الشخص ولقبه [4] ، وينقسم الاسم الى عدة اقسام :

- - الاسم الاصلي (الرسمي) هو(الاسم الذي يكتسبه الشخص عند ميلاده ويتم ذكره في بطاقة اهوية او غيرها من الاوراق والوثائق المتعلقة بالمعاملات الرسمية) [5].
- اسم الشهرة ويقصد به (ذلك الاسم الذي يطلقه الناس على الشخص ويشتهر به بينهم وعادة ما يستمد من احد الجوانب البارزة من مقومات شخصية الانسان او من طبيعة نشاطه الذي يمارسه في المجتمع لذلك فهو لايرد ذكره في شهادة الميلاد او بطاقته الشخصية) [6] .

---

[1] انظر نص المادة الثالثة من اللائحة الاوربية لحماية البيانات الشخصية .

[2] انظر المادة الثانية من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 .

[3] د. مروة زين العابدين صالح ، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت ، اطروحة دكتوراه ، كلية القانون جامعة عين شمس ، 2016 ، ص83 .

[4] د. وفاء حلمي ، محاضرات في نظرية الحق ، منشورات جامعة الزقازيق ، مصر ، 2007 ، ص68 .

[5] د. سهير منتصر ، النظرية العامة للحق ، منشورات جامعة الزقازيق ، مصر ، 2006 ، ص66 .

[6] د. سهير منتصر ، المصدر السابق ، ص 67 .

- الاسم المستعار وهو (اسم يتخذه الشخص لنفسه ليتخفى بعيدا عن اسمه الرسمي وذلك بمناسبة مباشرته عمل او نشاط معين مهني او فني او ادبي)[1].

واما اللقب فهو (اسم الاسرة التي ينتمي اليها الشخص وبالتالي فهو مشترك بين كافة افراد هذه الاسرة ، الا انه يختلف من اسرة الى أخرى) [2] .

واخيرا من الجدير بالذكر ان كلا من المشرعين العراقي والمصري قد اشار صراحة الى مفهوم الاسم وكذلك اشار المشرع المصري والاوربي في تعريفه للبيانات الشخصية الى الاسم بوصفه احد مصاديق هذه البيانات التي تسمح بتحديد الشخص الطبيعي المعني بها [3].

ب – العناوين الشخصية :.

يعد عنوان الفرد بيانا شخصيا ، سواء اكان عنوان سكنه الدائم او عنوان المكان المخصص لقضاء عطلاته واوقات فراغه او عنوان عمله او عنوان بريده العادي [4].

ج- السن او تاريخ الميلاد وشهادة الميلاد .

د – الارقام الشخصية :. يعد من قبيل البيانات الشخصية اي ارقام يتم منحها للشخص الطبيعي بحيث تكون خاصة به هو فقط ومميزة له ومحددة لهويته وقد ذكر كل من المشرعين الاوربي والمصري هذه الصورة بشكل صريح في تعريفهما للبيانات الشخصية وذلك تحت مسمى (الارقام التعريفية) ومن هذه الارقام ما يلي :

- رقم تحقيقه الشخص (الرقم الوطني او القومي)
- رقم الهاتف
- رقم التأمين الاجتماعي
- رقم جواز السفر [5].

ه – الاصول العرقية والاراء السياسية والنقابية والمعتقدات الدينية : اذ اكد المشرع المصري صراحة على ان هذه البيانات تعد من قبيل البيانات الشخصية وذلك بنصه في المادتين (1- 12) من القانون المذكور وهو نفس ما ذهب اليه المشرع الاوربي من المادة الرابعة من اللائحة (G D P R) .

و – الصوت والصورة :. تعد صورة الشخص الطبيعي بيانا شخصيا يندرج في نطاق البيانات الشخصية المشمولة بقانون حماية البيانات الشخصية ، ويستوي في ذلك ان تكون هذه الصورة ثابتة او متحركة (فيديو) لانها تسمح لتحديد هوية صاحبها بطريقة مباشرة ، كما تخضع صورة الشخص لنوع اخر من الحماية فيما يعرف بحق الانسان في صورته ، وعلى ذلك فمن الممكن منع الاعتداء على صورة الشخص

---

[1] د. سامح عبد الواحد التهامي ، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها ، مصدر سابق، ص 624 .

[2] د. سامح عبد الواحد التهامي ، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها ، المصدر نفسه ، ص625 .

[3] نص المادة (1/أولا) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 ، وكذلك المادة (1/4) من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016 .

[4] د. سامح عبد الواحد التهامي ، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها ، المصدر نفسه ، ص627.

[5] Nathalie Mallet . Poujol ,Protectionde lavie priree et desdonnres , Personnelles , p22 , etude disponible enlign a al adresse:https :\\eduscot , education fy\ Chrgt \ guideVie Privee . pif , le :18\3\2020.

، اما عن طريق قانون حماية البيانات الشخصية ، او بالحماية المقررة لحق الشخص على صورته في القوانين العقابية [1]. وان ما ينطبق على الصورة ينطبق على حديث الشخص او صوته ، فمن الممكن ان يكون مشمولا بحماية قانون البيانات الشخصية ، وخصوصا اذا كان هذا الصوت مميز واكتسب شهرة حقيقية به كما لو كان الشخص فنان او يعمل في مجال الانشاد .

2- البيانات الشخصية الصحية : لتحديد البيانات الشخصية الصحية فأنه يجب الرجوع الى المادة الرابعة من اللائحة (GDPR) للبحث فيها عن تعريف هذه البيانات وباستقراء التعريفات المذكورة في تلك المادة نجد انها قد اشتملت على تعريف للبيانات المتعلقة بالصحة وذلك على النحو الاتي :

(البيانات الشخصية المتعلقة بالصحة العضوية " البدنية او العقلية") لشخص طبيعي ، فضلا عن استعراض خدمات الرعاية الصحية التي تكشف عن المعلومات الخاصة بالحالة الصحية لهذا الشخص .

3- البيانات الشخصية المهنية : تعد البيانات التي تتعلق بالتاريخ الوظيفي للشخص بيانات شخصية كذلك الحال بالنسبة للبيانات المتعلقة باداءه الوظيفي ، ورقم تعريفه بالعمل والرواتب والاستحقاقات المادية والمعنوية والاجراءات الخاصة بالاختبار والتعيين والمراقبة اثناء العمل من خلال المكاتب ، والتليفون والبريد الالكتروني وغيرها [2] .

4- البيانات الشخصية المالية :. تعد كل البيانات التي تتعلق بحياة الشخص المالية او تعاملاته ، كدخله الشهري ونفقاته وديونه ، بيانات شخصية وكذلك الحال بالنسبة للحسابات البنكية [3] ، وارقام بطاقات الائتمان وبيانات القروض وتقارير الحسابات البنكية [4] .

ومما نخلص اليه في تحديد النطاق ان اي معلومة او بيان يتعلق بشكل مباشر او غير مباشر بشخص طبيعي محددا لهويته ، او من الممكن تحديده هو بيان شخصي يخضع للحماية القانونية للبيانات الشخصية ، وهذه الصور كما تم ذكره سابقا هي مجرد امثلة للبيانات الشخصية الاكثر شيوعا في الوقت الحالي، ففي الجانب العملي ان الكثير من المؤسسات والشركات الكبرى تجمع عن الافراد بيانات عديدة من هذا النوع تتعلق بالوضع المادي او الصحي او التعليمي او العائلي او العمل ، وتستخدم الكمبيوتر وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها ، وكذلك وفقا للمفهوم الحديث الذي اخذت به اللائحة الاوربية والمشرع المصري والتشريعات الاخرى ، وبالتالي فالمعيار هنا قابل للتطبيق على اي بيانات اخرى غير ما تم ذكره في النطاق الموضوعي والشخصي لهذه البيانات.

المبحث الثاني

اهمية البيانات الشخصية في مجال البيئة التجارية وآلية التعامل بها

قد تؤدي مشاركة البيانات الشخصية الى تحقيق فوائد ، وغالبا ما يكون من الضروري مشاركتها للتفاعل مع الاشخاص الاخرين في العصر الحالي ، وايضا هناك آلية تقنية وقانونية للتعامل مع هذه البيانات ، وهو ما سنتناوله في المطلبين الاتيين ، اذ سنتناول في المطلب الاول الاهمية الاقتصادية والقانونية للبيانات الشخصية ، وفي المطلب الثاني سنتناول آلية التعامل في البيانات الشخصية وكالاتي.

---

[1] د. حسام الدين كامل الاهواني ، مصدر سابق ، ص 76 .

[2] د. مروة زين العابدين صالح ، مصدر سابق ، ص 87 .

[3] د. سامح عبد الواحد التهامي ، مصدر سابق ، ص 631 .

[4] د. . نبيل محمد عثمان عرعارة ، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الالكتروني، ط1 ، المصرية للنشر والتوزيع ، القاهرة ، 2018 ، ص32

المطلب الاول

اهمية البيانات الشخصية

اثارت اهمية البيانات الشـــخصـــية الكثير من الخلاف وفيما اذا كانت لها قيمة مالية ام لا ، وكذلك فيما اذا كانت معالجتها وتداولها تمس في حياة الانسان وشخصيته ام لا ، وان هذا الاختلاف في حقيقته ناشئ عن تضاد في الاسس الفلسفية في البناء التشريعي للقوانين التي تعنى بتنظيم التعامل مع هذه البيانات والاولوية التي تعطيها قوانينها لهذه البيانات ، وهو ما ســـنتناوله تباعا في فرعين ، في الاول ســـنتناول القيمة الاقتصـادية للبيانات الشـخصـية ، وفي الثاني سـنتناول انعكاس القيمة الاقتصـادية على الاسـاس الفلسـفي للتشريعات المنظمة لحماية البيانات الشخصية وكالاتي :

الفرع الاول

القيمة الاقتصادية للبيانات الشخصية

انتشر التعامل بالبيانات الشخصية بشكل ملحوظ في العقود الاخيرة من القرن الماضـي ، وازداد الانتشار في هذا القرن بالتحديد ، حتى اصـبح يطلق على العصـر الحالي ب (العصـر الرقمي) نظرا للتطورات الكبيرة في مجال التكنولوجيا والاتصـالات ، وصـدرت بناء على ذلك العديد من التشـريعات التي تنظم ذلك الامر ، وتناول الفقه هذه البيانات بشـكل معمق ومن ضـمن ما تناوله مسـألة القيمة الاقتصـادية للبيانات الشخصية ، سواء لصاحبها او للشركة المستفيدة وكالاتي :.

اولا : القيمة الاقتصـادية للبيانات الشـخصـية بالنسـبة لصـاحبها : انقسـم فقهاء القانون بالنسـبة لتحديد القيمة الاقتصـادية للبيانات الشخصية ، وما اذا كانت تتمتع بقيمة مالية الى فريقين وكالاتي :

أ- الفريق الاول يذهب انصـاره الى ان البيانات ذات طبيعة خاصـة ولا يمكن اطلاق وصـف القيمة المالية عليها ، ولا تعتبر قيم يحميها القانون ولا يشـكل الاعتداء عليها مخالفة قانونية . اذ ان الاشـياء المادية هي من توصـف بالقيمة فقط ، انطلاقا من ان الاشـياء التي توصـف بالقيم هي الاشياء التي تقبل الاستحواذ عليها وتكون قابلة للتملك [1] . وعليه فانه لما كانت البيانات الشخصية ذات طبيعة معنوية لا يمكن الاستئثار بها ، فانها لا تدخل ضمن طائفة القيم المشمولة بالحماية ما لم تكن تنتمي الى مجموعة المواد الفنية والادبية والتي تحميها حقوق الملكية الادبية والفنية .

[1] محمد علي العريان ، الجرائم المعلوماتية ، اطروحة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2011 ، ص49 .

وعلى الرغم مما تقدم فقد ظهرت محاولات لانصـــار هذا الرأي المتقدم لتوفير الحماية القانونية للبيانات ، لذا فقد لجؤوا في بعض الاحيان الى استعمال دعوى المنافسة غير المشروعة ، والتطبيق الموسع لنظرية المنافسة الطفيلية ، ونظرية الاثراء بلا سبب ، واخيرا استندوا الى نظرية المسؤولية التقصيرية [1] .

ب- ويرى الفريق الثاني ان البيانات الشخصية في حقيقتها ذات قيمة مالية تتشابه في ذلك مع غيرها من القيم الاخرى [2] ، اذ يرى البعض بأن البيانات بذاتها قيمة مالية ويمكن ان تصـــبح قيمة قابلة للتملك في ذاتها بصرف النظر عن الوسيط المادي الذي يحويها ، وقد شبهها بالسلعة من حيث ان كليهما نتاج لعمل بشري وتنتمي الى من يحوز عناصرها بطريقة مشروعة ، ومن ثم يضعها في اي هيأة تكون معها صـــالحة للاطلاع عليها وتناقلها وتبليغها . وقد اســـتند هؤلاء الى حجتين رئيسيتين :

- الحجة الاولى : القيمة الاقتصادية للبيانات الشخصية والتي يمكن ان تقوم بالمال وبسعر محدد .
- الحجة الثانية : علاقة التبعية التي تربط البيانات بصاحبها وهي التي تربط المالك بالشيئ المملوك [3] .

ويرى الباحث صحة ما ذهب اليه الفريق الثاني ، خاصة في الوقت الحالي ، اذ تتمتع البيانات الشخصية بقيمة اقتصادية وتقوم بالمال مثلها مثل اي سلعة اخرى . واذا كان الكلام عن القيمة الاقتصادية للبيانات الشخصية بالنسبة لاصحابه ، فهل هذه القيمة تكون حاضرة بالنسبة للشركات التي تقوم بمعالجة هذه البيانات ، هذا هو ما سنبينه في النقطة ثانيا من هذا الفرع وكالاتي :

ثانيا : القيمة الاقتصادية للبيانات الشخصية بالنسبة للشركات التي تقوم بمعالجتها :. اذا كان موضوع القيمة الاقتصادية للبيانات الشخصية بالنسبة لاصحابها اثار جدلا بين القانونيين ، فان الامر مختلف هنا اذ من الثابت ان البيانات الشخصية المتدفقة عبر شبكة الانترنت الدولية على سبيل المثال تشكل عائد اقتصادي ضخم ومتراكم للشركات ، اذ تستخدم في تطوير وتنمية العديد من الخطط الترويجية والتسويقية لمنتجاتها المختلفة ، عن طريق جمع البيانات الشخصية للمستخدمين وتحليلها وتتبعهم قدر الامكان لمعرفة الاسلوب الاســـتهلاكي لهم و المواقع المفضـــلة لديهم ، و ذلك كله من خلال وضـــع قواعد بينات كبيرة وربطها بتفضيلاتهم واهتماماتهم ،وتقسيمها على اساس فئات اقتصادية او اجتماعية او عمرية وعلى هذا الاساس يتم تعيين الجمهور المستهدف بالحملات الترويجية للسلع والخدمات التي توفرها هذه الشركات او معرفة السلع الاستهلاكية لكل شخص لتطوير السلع والخدمات التي توفرها إضافة الى امكانية التصرف بقواعد البيانات التي تضم البيانات الشخصية الى شركات اخرى لتحقيق ارباح مادية[4] ، فمثلا تقوم الشركة الامريكية (Medical Marketing Service) ببيع بيانات الاشـــخاص الذين يعانون من عدة امراض وتضم قواعد البيانات هذه معلومات متعلقة بهؤلاء المرضى ك (العمر ، الجنس ، الدخل ، حجم الاسرة ، المستوى التعليمي ،والوضـــع الاجتماعي ، واســـلوب الحياة) ، وضـــمت هذه القوائم مرضـــى القلب

---

[1] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادية ، دار النهضة العربية ، القاهرة ، 2004 ، ص111 .

[2] د. وسيم شفيق الحجار ، النظام القانوني لوسائل التواصل الاجتماعي ، المركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية ، ط1 ، لبنان ، 2017 ، ص79 .

[3] د. نائلة عادل محمد فريد قورة ، مصدر سابق ، ص 115 .

[4] د. سارة الشريف ، خصوصية البيانات الرقمية ، الاصدار الثالث ، سلسلة اوراق الحق بالمعرفة ، مركز دعم لتقنية المعلومات ، القاهرة ، 2014 ، ص4.

والسكري وسرطان الثدي ،وايضا ما تذهب اليه الحكومة الهولندية في امكانية بيع البيانات الشخصية باعتبارها تشكل عائد مهم وهذا ما تبين في ما تسمعى بقضية (kvk)[1] ،

كما تقوم شركات اخرى ببيع قواعد بيانات تختص بما يفضل الاشخاص من كتب وعاداتهم الحياتية وحتى معتقداتهم الدينية [2] .

---

[1] تتلخص وقائع هذه القضية في تحقيق اجرته غرفة التجارة الهولندية عن إيرادات تجاوزت 3.3 مليون يورو في السنوات الست الماضية عندما جمعت وباعت تفاصيل الشركات ، معظمها لشركات تسويق مباشرة. كشف طلب حرية المعلومات (WOB) من قبل DutchNews.nl أن منتج مبيعات تم إيقافه ، بعد انتقادات من هيأة حماية البيانات الهولندية ، كان مربحًا. أدت خدمة Kamer van Koophandel (KvK) ´adressenbestand عبر الإنترنت ، التي تبيع كميات كبيرة من البيانات ، إلى شكاوى بشأن المكالمات المزعجة وانتهاكات الخصوصية ، لا سيما من العاملين لحسابهم الخاص. على الرغم من أن اللوائح الأوروبية الصارمة لحماية البيانات دخلت حيز التنفيذ في 25 مايو 2018 ، لم يتم سحب المنتج إلا بعد أكثر من عام. اذ التجار الفرديون ملزمون قانونًا بتسجيل بياناتهم لدى KvK. إذا لم يكن لديهم مكتب ، فعليهم تسجيل عنوان شخصي ، وإذا لم يكن لديهم خط أرضي ، رقم هاتف محمول: هذه متاحة للجمهور ، للدفع ، كجزء من قانون نزاهة الأعمال الهولندي. لكن مراقبي الخصوصية ومحامي الخصوصية أخبروا موقع DutchNews.nl أن KvK قد يواجه دعوى قضائية لخرق تاريخي لخصوصية بيع البيانات الجماعية ، ويستمر في انتهاك خصوصية المستقلين في رأيهم من خلال إنشاء إعلانات بيانات شخصية بواسطة جوجل ، وتم اخبار موقع DutchNews.nl أنه قد تكون هناك قضية مطالبة بالبيع الجماعي للبيانات ، بموجب قانون الناتج المحلي الإجمالي. تنص اللائحة العامة لحماية البيانات صراحةً على أن أي شخص عانى من ضرر مادي أو غير مادي نتيجة انتهاك يحق للائحة العامة لحماية البيانات (GDPR) تحكم بالتعويض من وحدة التحكم أو المعالج عن الضرر الذي لحق به. وأضافت أنه وفقًا للمادة 51 من السجل التجاري الهولندي لعام 2008 ، يحق للعاملين لحسابهم الخاص حماية عناوينهم إذا لم يكن لديهم خط أرضي مدرج في البورصة ، من بين عوامل أخرى. قانون الاتصالات الهولندي . اذ يتعين على الأشخاص في هذا المثال "الاشتراك" لتلقي مكالمات من مؤسسات مثل المسوقين عبر الهاتف. "حيث يبيع Kamer van Koophandel البيانات الشخصية للمتداولين الوحيدين ، يجب أن يكون لنشاط المعالجة هذا أساس قانوني ، كما هو مطلوب في اللائحة العامة لحماية البيانات ،" ومع ذلك خلصت AP [هيئة حماية البيانات الهولندية] إلى أنه لبيع منتجات أخرى غير "uittreksels" و "inzage" ، فإن الالتزام القانوني الذي يمكن أن يشكل أساسًا قانونيًا كما هو مطلوب في اللائحة العامة لحماية البيانات لا يمنع شيء موجود. و أدرجت KvK "الأضرار التي تلحق بالسمعة والمطالبات أو الغرامات" بسبب "تطورات البيانات المفتوحة" على رأس قائمة المخاطر التي تواجهها. ولا تهدف الوكالة من الناحية الهيكلية إلى الربح ولكنها تؤدي وظائف حكومية من خلال سن قوانين التجارة. وفقًا للتقرير ، كان لدى كبار الموظفين الأربعة حزم تعويضات سنوية تزيد قيمتها على 175000 يورو لكل عام. "كان هناك موقف قام فيه Kamer van Koophandel باعت البيانات بكميات كبيرة لشركات الطاقة ومراكز الاتصال المزعجة ". لقد تم إيقاف هذا ، وهو خبر سار . لكن هذا ليس سوى نصف القصة. اذ لا يزال بإمكان الجميع الحصول على التفاصيل الخاصة التي تخص العاملين لحسابهم الخاص والتجار الوحيدين ، والتي يمكن استخدامها للترهيب والمطاردة وغيرها من الأعمال الش ، وهذا ما يجب ايقافه. بحيث يمكن جعل السجل محميًا ولكن إذا كانت هناك حالة احتيال أو جريمة ، يمكن للشرطة رؤيتها ... وان مجموعة Concerns Bits of Freedom هي واحدة من مجموعة من المنظمات التي أثارت مخاوف بشأن انتهاكات الخصوصية ، مما أدى إلى مكالمات تسويقية مزعجة ، و أيضًا إلى مخاوف أكثر خطورة مثل التهديدات الموجهة إلى العاملين لحسابهم الخاص مثل الفنانين والصحفيين والكتاب. وان المواطنون الهولنديون قلقون للغاية بشأن الانتهاك المستمر للخصوصية وقالت وزارة الشؤون الاقتصادية الهولندية إنها بحاجة إلى العمل على تحقيق توازن أفضل بين الأعمال المفتوحة وحماية الحرية الفردية . قالت وزارة الشؤون الاقتصادية إن عناوين العاملين لحسابهم الخاص ستكون محمية في سجل الأعمال KvK (باستثناء الوكالات الرسمية مثل المحامين والمحضرين والهيئات الحكومية) في وقت لاحق من هذا العام. وأكدت متحدثة باسم KvK أن الهيئة تبيع تفاصيل من سجل الشركات من أجل جمع الأموال لتكاليف التشغيل الخاصة بها ، وهي ببساطة تنفذ القانون الهولندي ووظائفه القانونية ، على النحو الذي يجيزه القانون.

[2] د. توبي مندل و اندو بوديفات ، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير ، منشورات اليونسكو ، سلسلة اليونسكو لحرية الانترنت ، 2012 ، ص 16.

بيد انه اذا اعتبرنا المعلومات والبيانات الشخصية من قبيل القيم المعلوماتية ذات القيمة المالية التي تعطي لصاحبها حق معنوي مالي اشبه بحق الملكية كما رأينا سابقا ، فالسؤال الذي يطرح هنا عن المالك الحقيقي للبيانات الشخصية وفقا للتصور الخاص بالطبيعة المالية لها ، والذي يملك وحده حق استغلالها او استثمارها ؟.

اختلف الفقه في ذلك ، حيث ذهب البعض الى ان البيانات الشخصية للزبائن في الشركات المالية وكذلك المستخدمين في شركات الاتصال والتواصل بكافة تطبيقاتها وصورها ليست ملك لهؤلاء المستخدمين ، اذ ان قيمتها الاقتصادية او التجارية تكون لمن جمعها وحللها وعالجها ، باعتبار ان هذه الشركات تعرض خدمات مجانية غالبا ، لكنها عادة ما تتاح مقابل الاستخدام التجاري للبيانات الشخصية لهؤلاء الزبائن [1] ، الامر الذي يعني عدم تملك الزبائن للبيانات العائدة لهم ، ومن ثم لايحق لهم المطالبة باي حماية ، باعتبار ان حقائق المعلومات حسب هؤلاء تكون مستبعدة من نطاق الحماية بموجب قوانين الملكية الفكرية التي تحمي فقط الابتكار ، كما تستبعد ايضا من الحماية وفقا للقوانين المتعلقة بالاسرار التجارية التي تقتصر حمايتها على المعلومات التي تبقيها الشركات سرية اذا كانت لها قيمة تجارية او اقتصادية ، ولا تكون البيانات الشخصية لزبائن الشركات المالية وغيرها من الشركات من قبيل تلك المعلومات ، ومن ثم عندما تجمع هذه الشركات بيانات حول اهتمامات وميول الزبائن يكون لها وحدها امكانية المطالبة بملكية البيانات . ومن ثم عند طلبها الحماية لقواعد البيانات بما تضمه من بيانات شخصية باعتبارها ملكا لهذه الشركة وليس ملكا للزبائن [2] . وتحرص اغلب الشركات على النص ضمن الشروط التي تدرجها في الية التعامل معها على ان التسجيل من قبل الزبائن على الموقع هو بمثابة ترخيص باستخدام البيانات الشخصية اضافة الى المحتوى التجاري ، حيث يتم استخدام تلك البيانات ونشرها بدون علم الزبائن ، اضافة الى احقية احتفاظ الشركة بتلك البيانات وحق استخدامها وان انسحب الزبون لاحقا من التعامل مع الشركة [3] . كما ان بعض مواقع التواصل مثالها (تويتر) قد نص ضمن شروط استخدامه على انه في حالة بيع اصوله او دمجه او اعادة تنظيمه او الاستحواذ عليه ، فانه يمكن بيع البيانات المجمعة او نقلها في اطار العملية المنفذة .

وبذلك يرى انصار هذا الرأي ملكية هذه الشركات للبيانات الشخصية للزبائن ومستخدمي صفحاتها الالكترونية .

بيد ان جانبا اخر من الفقه يذهب الى ان ملكية البيانات الشخصية حق لصيق بشخصية اصحابها (الزبائن) وبالتالي فان ملكيتها لا تعود للشركات او غيرها ممن يملك مواقع الكترونية يمكنه الوصول الى بيانات زبائنه من خلال خدماته المقدمة ، حيث يستند هؤلاء الى النصوص القانونية التي حرصت على حماية اصحاب البيانات الشخصية عند معالجة تلك البيانات من قبل هيئات وجهات مختصة ، فالمادة (21) من اللائحة الاوربية للبيانات الشخصية تنص على انه " يحق للشخص المعني بالبيانات ان يعترض على معالجة بياناته الشخصية لاهداف الترويج التجاري " ومن ثم قد يؤدي الاعتراض لوقف المعالجة ، كما ان المادة الرابعة حظرت انشاء سيرة حول الشخص وحول حاجاته وميوله دون اذن خاص منه ، ويمتد الحظر ليشمل اي شكل من المعالجة الالية للبيانات الشخصية التي تتضمن استعمال هذه البيانات لتقييم

---

[1] Celine Castets-Renard , Droit de I Internet : Droit francais et europeen , 2eme edition , Montchrestien , L,extensor editions , 2012 , p 78.

[2] Lothar Deterinann , Social Media Privacy : A Dozen Myths and Facts , 2012 STANFORD Technology Law Review . 7. P 3 .

[3] Celine Castets – Renard , op cit , p 79 .

بعض جوانب الشخصية او مظاهر الشخصية المتعلقة بشخص طبيعي ، خاصة اي تحليل او تنبؤ لجوانب متعلقة في وضع الشخص الصحي او المالي او باداء الشخص بالعمل او مفضلاته وموقعه وتنقلاته [1] .

ويتضح من ذلك ان البيانات الشخصية بما أصبحت عليه هي غير قاصرة على قيمتها المعنوية بل تعدتها الى قيمة مادية تجارية او اقتصادية تعد ملكا لصاحبها ، فلا يجوز ان يتم تعميم تصنيفها او اتخاذ القرارات بشأنها دون موافقة مالكها ، فالتعميم وترتيب القرارات الهامة على اساسه قد يؤدي الى مزيد من الاشكاليات بالنظر لكون هذا التصنيف لا يعكس الا جانبا من شخصية الفرد ، وقد تشوبه الاخطاء وعدم الدقة حول حقيقة ما يحتويه من بيانات ، الامر الذي يمثل انتهاكا للحياة الخاص للزبائن [2].

ويرى الباحث صحة ووجاهة الرأي الثاني ، حيث ان تضمين الشركات المالية وغيرها من الشركات المختصة لشروط تحفظ لها حق استغلال او استعمال البيانات الشخصية للزبائن ، يجب ان لا ينصرف معناه الى ملكيتها لها ، اذ ان تلك البيانات تبقى ملكا خالصا لمن تمثله ، اذ لا يجوز لها التعامل فيها او استغلالها الا من خلال اذنه ، كما ان فرضية موافقة الزبون باستغلال بياناته ، ليس من شانها ان ينقل ملكية البيانات الى الشركة او ان تسلب ممن تمثله البيانات حق ملكيتها ، فثمة فارق كبير بين حق الملكية وحق الاستغلال باعتباره احد سلطات المالك و عناصر الملكية ، والذي يمكن ان يباشره المالك بشخصه او يعطي لغيره حق استعماله او استغلاله دون ان يسلبه ذلك الترخيص بالاستعمال او الاستغلال ملكية الرقبة المتمثلة في ملكية البيانات الشخصية لهذا الزبون .

الفرع الثاني

انعكاس القيمة الاقتصادية على الاساس الفلسفي للتشريعات المقارنة

رأينا ان البيانات الشخصية لم تعد كما كان عليه الحال سابقا ، اذ اصبحت تمثل قيم اقتصادية وتجارية مهمة ، تمثل سلع رائجة للشركات ، وخصوصا بعد الثورة الهائلة في مجال التكنولوجية والمعلومات ، اذا لا يكاد يكون هناك مجال في الحياة بعيد عن الانترنت بحيث يمكن النظر الى الانترنت على انه شبكة عالمية ، تبقى العديد من عناصر قانون الانترنت محددة من قبل الدول ذات السيادة ، وممكن ان يؤدي ذلك الى احتمالية الصراع التنظيمي والتوسع على وجه الخصوص ، والحكومات الوطنية لديها وجهات نظر مختلفة بشأن تنظيم البيانات الخاصة ولمن يجب ان تكون متاحة ، وهناك مخاوف بشأن كيفية التعامل مع البيانات الشخصية ، وتعد الولايات المتحدة الامريكية والاتحاد الاوروبي اكبر شريكين تجاريين لبعضهما البعض ، لكنهما يتبعان نهجا مختلفا الى حد كبير في محاولات كل منهما لتنظيم البيانات الشخصية والاقتصاد الرقمي ، ويستكشف الباحث هنا التباين العابر للحدود في سياسة الخصوصية في كل من الولايات المتحدة والاتحاد الاوربي ويناقش كيف ان الاختلاف في قيم البلدان والاعراف الاجتماعية والمصالح تفسر التباين في التنظيم [3]، اذ يهتم الاتحاد الاوربي بشدة على العديد من المجالات ، وان العصر الرقمي يتميز بتوافر وانتشار منتجات وخدمات الاتصالات الالكترونية ، هذه التطورات التي تجسدها الزيادة الكبيرة في سرعة وكفاءة المعاملات لتحفيز الانتاجية والنمو الاقتصادي ، اذ تنص لجنة

---

[1] د. وسيم شفيق الحجار ، النظام القانوني لوسائل التواصل الاجتماعي ، ط1، المركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية ، بيروت ، 2017 ، ص79 .

[2] Guillaume Florimond ,Droit et Internet , De la logique Internationaliste a la logique realiste , Bibliotheque des theses Editions Mare & martin , 2016 , p 340-341 .

[3] Janos Meszaros, 'Two Different Approaches of the Data Protection Law: the European Union and the United State' (2015) 9(1) Journal of Legal and political Sciences 1, 12

الاتصـالات الامريكية Federal Communications Commission (FCC)على ان الانترنت يلعب دورا مهما في الاقتصاد كمحرك لنمو الانتاجية وتوفير التكاليف ، اذ ارتفعت المعاملات التجارية والتجارة الالكترونية بشـكل كبير على الانترنت وخصـوصـا في العقود الاخير ، وتهتم التجارة بتبادل المعلومات والبيانات الشخصية مما يثير مشكلة حماية هذه البيانات والخصوصية في التجارة الالكترونية ، وقد يبدو ان تدفق البيانـات عبر الانترنت تؤدي الى الغاء الحدود الوطنية ، ومع ذلك لا تزال السـلطة القانونية والقضـائية المقيدة باقليم دولتها موجودة ، بينما يمكن النظر الى الانترنت على انه شـبكة عالمية ، الا ان الحكومات الوطنية لديها وجهات نظر مختلفة حول نوع المعلومات التي يجب ان تكون متاحة بشـكل قانوني وان يتم تنظيمها وفقا لذلك ، وهناك اشكالية شأن كيفية التعامل مع البيانات الشخصية ، بما في ذلك العمر والتوجه السـياسـي والديني ، والوضـع المالي والسـجلات الطبية والمعرفات مثل بطاقات الائتمان ورخص القيادة وجوازات السـفر والضـمان الاجتماعي وارقام الحسـابات المصـرفية / ومن يقوم بذلك ، وعلى الرغم من ان التعاريف الصريحة للخصوصية والبيانات الشخصية تختلف بحسب السياق ،حيث يتم تفسير الخصوصية وحماية البيانات الشخصية عادة من حيث معايير معالجة ونشر الانواع المذكورة اعلاه من المعلومات الشخصية . ومن المعلوم ان الرغبة في حماية البيانات الشخصية ليست ظاهرة جديدة ومع ذلك تؤثر التكنولوجيا الرقمية على الخصـوصـية بطرق جديدة من خلال جعل جمع البيانات والبحث فيها وخزينها وتجميعها وتداولها اسـهل وارخص ، مع اجراء المزيد من التعاملات عبر الانترنت ، وظهرت مشاكل الخصوصية الالكترونية الجديدة في هذه البيئة الشبكية ، فعلى سبيل المثال حدثت زيادة مؤخرا في استخدام الحوسبة حيث ترسل المؤوسسات العامة والخاصة بيانات الزبائن الخاصة بها الى طرف ثالث للتخزين والتأمين عليها ، ويتم تخزين بيانات الزبون في خوادم الانترنت ، وهو تطور دخل مؤخرا في النقاش الفقهي والاختلاف التشريعي من حيث مخاوف الامان والخصوصية ، في الوقت الذي تسعى فيه الدول الى السيطرة ومن خلال التنظيم تتفاقم قضية السيادة الوطنية والتحكم في حماية البيانات بسبب الانترنت ، حيث تتخطى البيانات الشخصية الحدود بسهولة في شكل رقمي ، وهناك تعارض بين المجال الاقتصادي لتدفقات البيانات عبر الحدود والاختصاص الاقليمي للتنظيم الوطني لخصوصية البيانات [1]، اذ يكون تدفق البيانات في شـبكة عالمية وفضـاء واسـع من التدفقات ، في حين ان تنظيم الدولة مرتبط بالجغرافية الى حدا ما ، ويبدو ان بعض خصـائص الانترنت تجعل هذه التكنولوجيا بلا حدود ، مما دفع المفكرين والفقهاء في نهاية القرن الماضـي وبداية الالفية الجديدة الى اقتراح انه لاي مكن التحكم في الانترنت وانه سـيؤدي الى تأكل السـلطة الوطنية ، ومع ذلك فأن العديد من اقليميتنا السـياسـية العالمية وخاصة الانظمة القانونية لا تزال محددة من حيث الدول ذات السيادة ، والدول التي تملك السلطة في تنظم الانترنت وهذا يخلق تناقضا متأصلا يتفاقم بسبب الاساليب المختلفة الى حد كبير كالتي تستخدمها الدول في محاولتها تنظيم الانترنت والتجارة الالكترونية وهو ما يمكن تلمسـه في دول الاتحاد الاوربي من جهة والولايات المتحدة الامريكية من جهة ثانيا وكالاتي .

ففيما يخص الاتحاد الاوربي وان كان قد نظم بشكل استباقي استخدامات البيانات الشخصية ، فقد امتنعت الولايات المتحدة الامريكية عن التنظيم لحماية البيانات الشخصية ، ومع ذلك تصبح الاختلافات التنظيمية إشكالية قانونية عندما تتعدى العلاقات القانونية حدود الدولة الواحدة ، اذ قد تؤثر القوانين واللوائح الوطنية لحماية البيانات الشـخصـية احادية الجانب على انشـطة الانترنت للمسـتخدمين في دول اخرى ، وتخلق التداعيات التنظيمية والاختلافات في السياسة بيروقراطية مهدرة وارتباكا واوجه قصور للبلدان والشركات

[1]Lauren Movius and Nathalie Krup, 'US and EU Privacy policy: Comparison of regulatory Approaches' (2009) International Journal of Communication,p; 187.

المعنية وكذلك للجمهور ويمكن للتأثير التنظيمي المفرط في الولايات المتحدة والاتحاد الاوربي ان يعطل كلا الاقتصادين ، اذ تشكل التجارة بين هاتين المنطقتين ما يقرب من 40% من التجارة الدولية حسب المديرية العامة للتجارة في المفوضية الاوربية عام 2007 ، علاوة على ذلك تعتبر التجارة الالكترونية عنصرا مهما بشكل متزايد في هذه التجارة والاستثمار في الواقع الاقتصادي العالمي ، وتشكل الاختلافات التنظيمية بين الولايات المتحدة الامريكية واوروبا في هذه البيئة الرقمية تحديات للحكومة والجهات الفاعلة الخاصة في كل النظامين ، وحماية البيانات الشخصية هي احدى هذه القضايا التي تتطلب الاهتمام ، ويزيد انتشار الانترنت وجمع البيانات الالكترونية من احتمالية تعرض خصوصية البيانات للخطر [1]، ومع ذلك وكما تم ذكرهٍ فان الحماية القانونية للبيانات الشخصية تختلف اختلافا كبيرا في اغلب بلدان العالم وفي العديد من المجالات ، اذ لا يتم النظر في خصوصية البيانات بشكل مستقل فدائما ما يتم النظر اليها في سياق اجتماعي وسياسي واقتصادي وثقافي وتاريخي محدد ، وبالتالي فأننا نقارن بين مفاهيم البيانات والخصوصية في السياقين الاوربي والامريكي وتأثير الاختلاف على التشريعات القانونية في كلا المنطقتين وكالاتي :

اولا : الاختلاف الفلسفي في تحديد معنى الخصوصية :. يمكن اعتبار معايير الخصوصية المختلفة في الولايات المتحدة الامريكية والاتحاد الاوربي نتيجة طبيعية للخلافات بشأن دور الحكومة والقطاع التجاري بشكل عام ، اذ يتطلب النهج الاوربي في ادارة الشركات مشاركة وثيقة بينها وبين لحكومة لتحقيق المهام العامة ، وينظر الى الحكومة على انها شريك نشط الى جانب المشاركين الرئيسين في الصناعة ، حيث يناقشون الاهداف التنظيمية والمصلحة العامة والاستراتيجيات لتحقيقها ، علاوة على ذلك اتجه صانعوا القرار الاوربي الى رؤية دور اوسع للدولة في معالجة المشكلات الاجتماعية[2] بالمقابل فضل صانعوا القرار الامريكي نهج عدم التدخل في ادارة الشركات والتأكيد على دور الجهات الفاعلة الخاصة وقوى السوق في تحقيق التحديات المجتمعية . وان هذا التصوير لهذه الاساليب التنافسية هو تجريدات لمجموعة السياسات المعقدة والديناميكية التي يتم تصويرها بشكل افضل في مجملها كنقاط نسبية على المجموع بدلا من الاضداد المجتزأة ، وان المحاولات الاوربية لتنظيم الخصوصية تبع ايضا من مفهوم الخصوصية لديهم ، اذ ان الاوربيين يعتبرون الخصوصية حقا اساسيا من حقوق الانسان والتي تتحمل الحكومة مسؤولية توفيرها لمواطنيها ، وهذا الحق مذكور صراحة في دساتير العديد من دول الاتحاد الاوربي بما في ذلك المانيا واسبانيا وغيرها ، وفي اتفاقية مجلس اوروبا لحماية حقوق الانسان والحريات الاساسية [3].
وايضا على المستوى التاريخي ترتكز حماية البيانات على محاولات الدول الاوربية للتحكم في الاستخدام غير السليم للبيانات الشخصية ، اذ هناك رغبة عندهم في التعافي من الفكر النازي والكي جي بي السوفيتي ، ويظل الاوربيون على درجة عالية من الحساسية تجاه جمع ملفات البيانات الشخصية . ومن خلال ماذكر نلاحظ ان قيمة استخدام المعلومات لتعزيز التجارة الاستهلاكية اقل اهمية في الاتحاد الاوربي منها في الولايات المتحدة ، والتي تتمتع باقتصاد يحركه المستهلكون فعلى سبيل المثال المتاجر في الولايات

---

[1] د. كريم محمد محي الدين سليم ، نطاق الحق في الخصوصية ومدى تأثره بالتقنيات الحديثة ، اطروحة دكتوراه مقدمة الى كلية الحقوق جامعة المنوفية ،2018، 275 .

[2] Michelle Goddard, 'The EU general Data Protection Regulation (GDPR): European Regulation That has a Global Impact' (2017) 59(6) International Journal of Market Research 703, 705

[3] تنص اتفاقية تاسيس دستور لاوروبا صراحة على ضرورة تعزيز حماية الحقوق الاساسية في مجموعة التغييرات في المجتمع والتطورات التكنولوجيا ، وايضا تضمن المادة 8 من الاتفاقية الاوربية لحقوق الانسان الحق في احترام الحياة الخاصة والعائلية والمنزل والمراسلات.

المتحدة غالبا ما يكون لديهم ساعات طويلة بينما قد يواجه تجار التجزئة في الاتحاد الاوربي قيودا صارمة على ساعات العمل . وتشير الاحصاءات الى ان الاتحاد الاوربي لديه بطاقة أئتمان واحدة تقريبا لكل اربعة اشـــخاص [1]، بينما لدى الولايات المتحدة 2:25 بكاقة ائتمان لكل شـــخص ، وتتجاوز مدخرات الاتحاد الاوربي 10% من الدخل الفعلي ، بينما يكون متوسط مدخرات الولايات المتحدة من الدخل بحدود الصفر او يكون سـالبا عند التمويل عن طريق الاقتراض ، حتى انهيال قطاع الاسـكان والائتمان عام 2007 كان كثير من ثروة امريكا يسـتثمر في الاسـهم العقارية ، واما حاليا فهناك نسـبة كبيرة ومتنامية من الامريكين لـديهم ديون عقـاريـة تتجـاوز قيمـة ممتلكـاتهم ، وهنـا من المهم الملاحظـة ان الاتحـاد الاوربي والولايـات المتحدة كلاهما بعيد كل البعد عن التوحيد ، وايضا من الملاحظ ان النهج التنظيمي للاقتصاد والحكومة في المملكـة المتحـدة اقرب الى حـالة الولايات المتحدة من معظم دول الاتحاد الاوربي ، وان توجيه اللوائح في الاتحاد الاوربي يمثل توجيه لحماية البيانات الشـخصـية في الاتحاد والتركيز على حماية الخصـوصـية في اوروبا ، اذ اصدر الاتحاد الاوربي توجيها شاملا لحماية البيانات ينطبق على معالجة المعلومات الشخصية في الملفات الالكترونية واليدوية ، وسـعى هذا التوجيه الى تنسـيق قوانين الدول الاعضـاء الخمسـة عشـر انذاك في توفير مسـتويات متسـقة من الحماية للمواطنين وضـمان التدفق الحر للبيانات الشـخصـية داخل الاتحاد الاوربي ، ويعزز التجارة داخل اوروبا ، ويضع مستوى اساسيا مشتركا للخصوصية لا يعزز فقط قوانين حماية البيانات الحالية ولكن تنشـــئ ايضـــا مجموعة من الحقوق الجديدة ، ويفترض التوجه تدفق البيانات عبر الحدود ويحاول حماية حقوق خصـوصـية البيانات للاوربيين فيما يتعلق بالمكان الذي يتم فيه نقل البيانـات ومعـالجتهـا [2] ، اذ تنص المادة (25) من التوجه على ان الدول الاعضـــاء تضـــمن حماية البيانات الشـــخصـــية المتعلقة بالمواطنين الاوربيين عند تصـــديرها ومعالجتها في بلدان خارج اوروبا ، وكذلك تلتزم الدول الأعضـــاء على انه في حال نقل البيانات الشـــخصـــية التي تخضـــع للمعالجة او المعدة للمعالجة بعد النقل الى بلد ثالث لا يتم الا اذا ضـمنت الدولة الثالثة المعنية مسـتوى مناسـبا من الحماية مع مسـتوى الحماية المناسـب الذي تم تقييمه في ضـوء جميع الظروف المحيطة بعملية نقل البيانات . ويجب ايلاء اعتبـار خـاص لطبيعـة البيـانـات والغرض من عمليـة المعـالجـة المقترحـة او العمليـات ومدتهـا ، وبلد المنشـأ وبلد المقصـد النهائي وقواعد القانون العام والقوانين القطاعية السـارية في الدولة الثالثة المعنية ، والقواعد المهنية والتدابير الامنية التي يتم الالتزام بها في ذلك البلد [3]، وعلى الرغم من ذلك ادرج الاتحاد الاوربي استثناءات بموجب المادة 26 من خلال السماح بنقل البيانات الى البلدان التي لم تعتبر فيها الحماية كافية على امل تغطية عمليات نقل المعلومات اليومية ، مثل معلومات سفر الركاب ، ، وسرعان ما اصبح واضـحا ان التجارة وتدفقات البيانات بين الولايات المتحدة والاتحاد الاوربي لن يتم ضـمانها على اسـاس اعفاءات المادة 26 وحدها ، وان المفوضـــية الاوربية لن تقبل نظام الرقابة على الحجز الامريكي الحالي باعتباره ملائما ، وفي نهاية 1998 بدأت المفاوضـــات بين الجانبين مما ادى في النهاية الى انشـــاء اتفاقية الملاذ الامن ، وتم اعتمادها عام 2000 وتتطلب الامتثال الى ســـبعة مبادئ ، (الاشـــعار ، الاختيار ، الانسحاب عند النقل الى طرف ثالث ، الوصـول الى معلومات الفرد ، حماية وامن المعلومات الشخصية ، سلامة البيانات ، الانفاذ) ويعتبر قانون الملاذ الامن عملية مبسطة للشركات الامريكية للامتثال لتوجيهات الاتحاد الاوربي ، وعلى الشركات الامريكية التي تتعامل مع البيانات الشخصية لمواطني الاتحاد الاوربي

---

[1] Janos Meszaros,op-cit,p9.

[2] The EU's General Data Protection Regulation (GDPR) was adopted on 8 April 2016 and came into force until 25 May 2018.

[3] Mark Phillips, 'International Data-Sharing Norms: from the OECD to the General Data Protection Regulation (GDPR)' (2018) 137(8) Human Genetics,p; 575, 582

التسجيل طواعية لتجنب عقوبات الاتحاد الاوربي .وبالتالي فأن الشركات التي اشتركت في هذه الاتفاقية تعتبر انها توفر حماية كافية لبيانات مواطني الاتحاد الاوربي ، ولم يتأثر اي من الطرفين بهذه الاتفاقية ، ولكن يعتقد الاوربيون انه لايمكن ان يقترب من تقديم مستويات كافي من الحماية الحقيقية ، بينما تعتقد امريكا ان التنفيذ و التشغيل سيكونان مكلفان للغاية [1]، واوضحت مفاوضات الملاذ الامن الاختلافات العميقة الجذور في الخبرة التاريخية والقيم الثقافية والمعتقدات حول تنظيم الدولة والاقتصاد والمجتمع والشفافية وامكانية انفاذ سياسات الخصوصية ، ونشأت مشاكل فيما يتعلق بعمليات النقل اللاحقة وحالة الاطراف الثالثة ، وتساهم هذه التناقضات التنظيمية والخلاف القانوني المتزايد بين الولايات المتحدة والاتحاد الاوربي في عدم الكفاءة التنظيمية حول معايير خصوصية الانترنت .

ففي الوقت الذي تخضع فيه حماية البيانات الشخصية الى التنظيم الشديد في اوروبا ، فانه في درجة اخف في الولايات المتحدة الامريكية ، اذ على المستوى التاريخي كانت الولايات المتحدة تتبع تقليديا نظام عدم التدخل ، حيث تحدد الاسواق اجندة الصناعة ، وتدخل الحكومات فقط حينما يفشل القطاع الخاص ، ففي العديد من قطاعات الاقتصاد الامريكي كان دور الحكومة هو ان تكون صانع قواعد كملاذ اخير ، ولا يحتوي دستور الولايات المتحدة الامريكية على كلمة خصوصية وبالتالي فان الحق في الخصوصية لا يضمنه الدستور . اذ جاء مفهوم الخصوصية عندهم من مقالات بعض المحامين الامريكيين حول الحق في الخصوصية كاجراء تقصيري حيث عرف صراحة الخصوصية على انها " الحق في ان تترك وشأنها " وظهر مفهوم الضرر المتعلق بالخصوصية تدريجيا كجزء من القانون في جميع انحاء الولايات المتحدة الامريكية وساعد في تكوين فكرة ان الخصوصية هي سلعة واداة في الاساس ضد الحكومة ، وحماية البيانات الشخصية في القانون التشريعي في الولايات المتحدة ليست متطورة بشكل جيد على عكس الاتحاد الاوربي[2]، اذ لايوجد قانون شامل واحد ، الا ان هذا لا يعني ان القانون الفيدارلي اهمل القضايا القانونية في اطار البيانات الشخصية اذ اعترفت المحكمة العليا الامريكية عام 1965 بالحق الضمني للفرد في الخصوصية فيما يتعلق بالحكومة في قضية الغاء تجريم استخدام وسائل منع الحمل . وايضا نظمت الحماية القانونية لخصوصية المعلومات في القطاع الخاص في عدة قوانين [3]. ويلاحظ مدى صعوبة مقارنة شبكة قوانين الولايات المتحدة معايير الاتحاد الاوربي ، وفي الوقت الذي تدرك فيه الولايات المتحدة اهمية حماية الخصوصية من اجل نمو التجارة الالكترونية ، وتواصل التنظيم الذاتي في مختلف الصناعات اذ ان القطاع الخاص يلعب دورا رائدا في التجارة الالكترونية ، ولكن وفقا للسياسة التشريعية الامريكية يتم الاعتماد على التنظيم الذاتي في ادارة مخاوف الخصوصية وترك التجارة الالكترونية للتنظيم الذاتي قدر الامكان ، وهذا ما تفضله معظم الشركات الامريكية ، وقد سعت هذه الشركات الى تنظيم نفسها من خلال اليات مختلفة ، مثل شفرات الصناعة ، والمنظمات كتحالف الخصوصية عبر الانترنت الذي تم تطويره في عام 1988 . وفي الحقيقة هذا النهج يتناقض مع مع سياسة الاتحاد الاوربي لخصوصية البيانات ، اذ في اوروبا تقع على عاتق الحكومة مسؤولية حماية حق المواطنين في الخصوصية ، بينما في امريكا الاعراف والتعاقدات وليس القانون يشكلان نطاق الحماية لتلك البيانات وخصوصيتها ، وفي

---

[1] Rikke Jorgensen, 'Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google' (2017) 35(2) Nordic Journal of Human Rights, p; 126

[2] Clair Laybats and John Davies, 'GDPR: Implementing the Regulation' (2018) 35(2) Business Information Review , p ; 81, 83

[3] مثل قانون الابلاغ عن الائتمان العادل لعام 1970 وقانون حماية خصوصية الفيديو لعام 1988، وقانون حماية المستهلك والمنافسة في تلفزيون الكابل ، وقانون حماية خصوصية الاطفال على الانترنت وغيرها من القوانين في كل ولاية على حدة .

الاتحاد الاوربي ينظر الى البيانات الشخصية بوصفها من حقوق الانسان الأساسية ، اما في الولايات المتحدة ينظر الى الخصوصية بوصفها سلعة تخضع لاعراف ومعايير السوق ويتم تصويرها من الناحية الاقتصادية[1] .

ويذهب البعض الى انه هناك فوائد واضحة لحماية الخصوصية ، ولكن ايضا هناك تكاليف ذات صلة ، اذ يمكن ان تفرض الخصوصية تكاليف اقتصادية وقيود اجتماعية ، في حين ان الخصوصية قد تحمي بعض الافراد ، الا انها قد تؤدي الى تكاليف من خلال منع الاخرين من اتخاذ قرارات مدروسة ، وفي الوقت الذي تتحرك فيه البلدان لتأمين حماية الخصوصية لمواطنيها ، فانها تضطر الى اعطاء الاولوية بين قضايا الخصوصية والامن والكفاءة الاقتصادية ، ويؤثر موقف الحكومات تجاه هذه التوازنات على طريقة عمل الطرفين ، ويمكن للحكومات التلاعب بالعلاقة الضمنية والصريحة بين الخصوصية والكفاءة الاقتصادية والامن لتحقيق اهداف مختلفة . وسيتم كشف التعارض بين حماية الخصوصية والكفاءة الاقتصادية ، والتصادم بين بين حماية الخصوصية والامن من جهة اخرى . و من امثلة التعارض الاقتصادي ان المشترين يريدون ان يعرف البائعون ذوقهم والمنتج الذي يريدونه ، مما يقلل من تكاليف البحث عن المنتج المناسب ، ومع ذلك لايريد المشتري ان يعرف البائع الحد الاقصى للسعر الذي يرغب في دفعه مقابل السلعة [2]. وتشير الابحاث الاقتصادية الى انه عند توفر معلومات حول اذواق الزبائن وتاريخ الشراء ومشاركة بين البائعين تنتج الاسواق نتائج فعالة يستفيد المشتري من الخدمات المستهدفة التي تقلل تكاليف البحث ، بينما يستفيد البائع من تصحيح المعلومات غير المتماثلة حولة تفضيلات المشترين .ويسمح التهرب من الخصوصية بالنسبة للبائع معرفة المزيد من رغبة الزبائن مما يحقق منفعة حقيقية له .اما على مستوى التعارض بين الخصوصية والامن فان هناك من يذهب الى المجتمعات الديمقراطية تسعى الى تحقيق توازن بين الجاذبية والامن ، وانه يجب على المواطنين التخلي عن درجة معينة من الخصوصية الشخصية من اجل الامن ، فبعد احداث الحادي عشر من سبتمبر والحرب على الارهاب اكتسبت قضية الامن مقابل الخصوصية هذه اهمية جديدة ، وهناك من اعترض على ذلك بقوله ان " هؤلاء الذين يمكنهم التخلي عن الحرية الاساسية للحصول على امان مؤقت لا يستحقون الحرية والامان " . اذ غالبا ما تتم مناقشة الامن والخصوصية وان التخلي عن الخصوصية لا يؤدي بالضرورة الى مزيد من الامان ، وان الامن الاكبر لا يتطلب فقدان الخصوصية . ونلاحظ هنا انه غالبا ما يتم النقاش على انه الامن مقابل الخصوصية ، ولكن في توجه اخر ذهب الى ان الحقيقة هو الخصوصية مقابل السيطرة ، اذ حظيت الامنية الوطنية او التوازن بين الخصوصية الفردية والتعامل مع المعلومات الشخصية التي تم جمعها مؤخرا لاسيما في الولايات المتحدة بعد تشريع قانون باتريوت ، في حين ان جمع المعلومات الشخصية وقواعد البيانات الحكومية يمكن ان توفر معلومات مفيدة اجتماعيا حول المنظمات والمؤسسات ، الا ان الاشكالية تثور عندما يمكن نشر هذه المعلومات او كيفية استخدامها .

ثانيا : تأثير الاختلاف على التشريعات الصادرة في الاتحاد الاوربي والولايات المتحدة :. يختلف مفهوم حماية الخصوصية وأهميته النسبية مقابل المنافع الاجتماعية الأخرى ، وأدوار الحكومة والمنظمات الأخرى في حماية المواطنين ، وتنفيذ اللوائح التنظيمية بشكل كبير عبر البلدان. و تساهم هذه المشكلات جنبًا إلى جنب مع المفاهيم المختلفة للخصوصية في الولايات المتحدة وأوروبا كما تمت مناقشته أعلاه ، في الحوكمة والتنظيم المتميزين اللذين يهدفان إلى تحقيق توازن الخصوصية في نقاط معينة لتحقيق

---

[1] Phillips,op-cit,p 6.

[2] Clair Laybats and John Davies,op-cit,p 87.

أولويات متميزة[1]. يجسد توجيه الاتحاد الأوروبي في ترجيح الخصوصية مقابل الكفاءة الاقتصادية من خلال توضيح ميل أوروبا إلى امتياز حماية الخصوصية على حساب الوصول إلى البيانات والكفاءة الاقتصادية. يخلص الباحث إلى أن حماية حقوق المواطنين أو موضوعات البيانات الشخصية في أوروبا يتفوق على النتائج الاقتصادية للسوق[2]. تم تقديم التوجيه الاوربي كمحاولة لتأمين الحق الأساسي للخصوصية في جميع الدول الأعضاء. اذ بدا الاتحاد الأوروبي على استعداد للمخاطرة بخسائر اقتصادية ضخمة من خلال وقف تدفقات البيانات مع دول ، مثل الولايات المتحدة ، والتي لم توفر حماية كافية لمعلومات المواطنين الأوروبيين. و للإشارة إلى الخسائر الاقتصادية المحتملة الناجمة عن زيادة حماية الخصوصية ، أكد الشراح أن أي شركة تعمل داخل الاتحاد الأوروبي أو تتلقى معلومات منه سيتعين عليها مراجعة عمليات تسليم البيانات الخاصة بها، اذ لن تتمكن حينها الشركات من جمع البيانات من زبائنها والتصرف بها دون رضا منهم. وحينها يتعين على الشركات ، فيما يتعلق بالموقع ، أن تستحصل بشكل صريح الموافقة ، والمعروفة باسم "الاشتراك" ، [3] من جميع الزبائن والموظفين الأوروبيين لمجرد إدراج معلوماتهم في البريد الإلكتروني للشركة أو أدلة الهاتف على الرغم من هذه التكاليف المحتملة ، التي تزداد مع نمو القدرات الرقمية ، سعى الاتحاد الأوروبي إلى منح الأفراد حقوقًا في بياناتهم الشخصية. شرعت الولايات المتحدة قانون باتريوت بقصد زيادة الأمن القومي ، وبالتالي ألغت درجة معينة من حماية الخصوصية لمواطنيها. تبخر هذا المستوى من الحماية المحلية في 11 سبتمبر 2001 عندما أصبحت مدينتان أمريكيتان رئيسيتان أهدافًا لأعمال الإرهاب وأثرت بشكل كبير على الفكر الامريكي . ضمنت هذه الخلفية فعليًا أنه في ميزان الأمن مقابل الخصوصية ، ستكون السلطات الأمريكية لصالح الأول. بالإضافة إلى ذلك ، فإن النظام القانوني تاريخيًا للولايات المتحدة ، جنبًا إلى جنب مع النظرة التقليدية للخصوصية كسلعة ، جعل الولايات المتحدة أرضًا أكثر خصوبة لاعتماد التشريعات التي تفضل الأمن القومي على الخصوصية. وايضا التغييرات التقنية والمعقدة لقوانين المراقبة ولوائح الاحتجاز والمبادئ التوجيهية الحكومية التي تتجاهل الضوابط والتوازنات التقليدية وتزيد في نهاية المطاف من سرية الحكومة ، تعزز الآمال في الأمن القومي على حماية الخصوصية. تميل جميع هذه الإجراءات التشريعية إلى زيادة مراقبة الاتصالات ، وتكثيف مشاركة البيانات ، وزيادة مخططات تحديد الهوية. و كان الاتحاد الأوروبي يعمل على سن تشريع لمكافحة الإرهاب ، ولكن على عكس قانون باتريوت الأمريكي ، يبدو أن هناك ضوابط وضرورة اخذ التوازنات المعمول بها لحماية الحريات العامة وضمان ألا تدفع هذه الحريات ثمن زيادة الأمن العام. أصر أعضاء البرلمان الأوروبي على تضمين قواعد معالجة البيانات الشخصية ، من منطلق الإصرار على أن "العلاج لا ينبغي أن يكون أسوأ من المرض" [4]. وبالتالي ، فقد نظر صانعو السياسة الأوروبيون في تأثير التشريع على الإجراءات القضائية ، وهو نقاش يبدو أنه لم يحدث مع تمرير سريع لقانون باتريوت.

اما في اوروبا فقد تم تشريع اللائحة العامة لحماية البيانات رقم 679 لسنة 2016 والتي تطبق في جميع دول الاتحاد الأوروبي وتحل محل قوانين حماية البيانات المختلفة المعمول بها حاليًا في الدول الأعضاء المختلفة، اذ يوسع نظام حماية البيانات الجديد في الاتحاد الأوروبي نطاق قانون حماية البيانات في

---

(1) Lauren Moius & Nathalie Krup International Joumal of Communication 3 (2009) ,178

(2) Reidenberg , J,R .(2000) Resolving conflicting international data privacy rules in cyberspace.stanford law Review,52,1315-1371.

(3)Reidenberg , J,R,op-cit,p58

(4)EurActiv.com.(2008,sept.24). EU makes headway on anti-terror law.Retrieved Des .18,2008 , from.http://www.euractiv.com.

الاتحاد الأوروبي ليشمل جميع الشركات الأجنبية التي تعالج بيانات المقيمين في الاتحاد الأوروبي. ينص على تنسيق لوائح حماية البيانات في جميع أنحاء الاتحاد الأوروبي ، مما يلزم الشركات الأمريكية الامتثال لهذه اللائحة ومع ذلك ، فإن هذا يأتي على حساب نظام امتثال صارم لحماية البيانات مع عقوبات شديدة تصل إلى 2٪ من حجم المبيعات في جميع أنحاء العالم. "وايضا يتم تطبيق لائحة حماية البيانات الاوربية على جميع الشركات من خارج الاتحاد الأوروبي دون أي مؤسسة في الاتحاد الأوروبي ، شريطة أن تكون معالجة البيانات موجهة إلى المقيمين في الاتحاد الأوروبي[1]. اذ يجبر هذا على سبيل المثال الشركات الأمريكية ليس فقط على الامتثال لقانون الاتحاد الأوروبي ، ولكن أيضًا لإنشاء إدارة حماية البيانات ، على سبيل المثال من خلال تعيين مسؤول حماية بيانات "أوروبي". كقاعدة عامة ، تتطلب أي معالجة للبيانات الشخصية تقديم معلومات واضحة وبسيطة للأفراد المعنيين بالإضافة إلى الحصول على موافقة محددة وصريحة من هؤلاء الأفراد لمعالجة بياناتهم ، بخلاف الحالات التي يسمح فيها نظام حماية البيانات صراحة بمعالجة البيانات الشخصية. اذ تشترط اللائحة نقلًا آمنًا للبيانات خارج الاتحاد الأوربي ، و نظمت اللائحة حقوق خصوصية جديدة مثل "حق قابلية النقل" لموضوع البيانات و "الحق في النسيان" ، في الاتحاد الأوروبي. سيسمح "حق قابلية النقل" بنقل جميع البيانات من مزود إلى آخر عند الطلب ، على سبيل المثال نقل ملف تعريف وسائط اجتماعية أو بريد إلكتروني "[2].

تؤثر اللائحة الاوربية العامة لحماية البيانات الشخصية أيضًا بشكل غير مباشر على جميع الشركات التي لديها شركاء تجاريون وموردون في دول الاتحاد الأوربي لأنهم ممنوعون من إرسال البيانات الشخصية. "ترغب مقرات الشركات متعددة الجنسيات في التحكم في العمليات على مستوى العمل من خلال جعل عملية صنع القرار ومعالجة البيانات مركزية لأنها أكثر سرعة وفعالية من حيث التكلفة. وهناك الكثير من الخيارات والحلول لإرسال البيانات الشخصية إلى الشركات المقيمة في بلدان ثالثة غير كافية من وجهة نظر قانون حماية البيانات في الاتحاد الأوروبي: (موافقة صاحب البيانات ، الضرورة بموجب العقد ، الاهتمام بموضوع البيانات، الضرورة بموجب القوانين ،الملاذ الآمن ، قواعد الشركة الملزمة وايضا اتفاقية نقل البيانات) وتم إنشاء لجنة (EDPS) بموجب اللائحة رقم 2001/45. "تتمثل المهام الرئيسية لهذه اللجنة في مراقبة معالجة البيانات الشخصية من قبل دول الاتحاد الأوروبي ، وتقديم المشورة بشأن السياسات والتشريعات التي تؤثر على الخصوصية ، والتعاون مع السلطات المماثلة من أجل ضمان حماية متسقة للبيانات . كما أنه يراقب التقنيات الجديدة التي قد يكون لها تأثير على حماية البيانات. تتمثل المهمة الأكثر أهمية للجنة الاشراف على البيانات الشخصية التي تتم معالجتها من قبل مؤسسات وهيئات الاتحاد الأوروبي ". يقوم بإجراء "فحص مسبق" عندما تقوم مؤسسات وهيئات الاتحاد الأوروبي بعمليات معالجة البيانات الشخصية ذات المخاطر المحددة. يمكن لـ EDPS تقديم المشورة عندما يتلقى شكوى من موظفي الاتحاد الأوروبي أو من أشخاص آخرين حول إساءة التعامل مع بياناتهم الشخصية من قبل مؤسسة أو هيئة تابعة للاتحاد الأوروبي. يمكنه أيضًا تقديم المشورة بمبادرة منه. وتتشاور اللجنة مع المشرعين في الاتحاد الأوروبي حول مقترحات التشريعات الجديدة وأدوات القانون غير الملزم التي يمكن أن تؤثر على حماية البيانات الشخصية. يغطي التعاون قضايا محددة مثل تفسير توجيهات الاتحاد الأوروبي لحماية البيانات ، بالإضافة إلى المزيد من التعاون الهيكلي مع سلطات حماية البيانات الأخرى. يمكن لـ EDPS أيضًا التدخل في القضايا المعروضة على محكمة العدل والمحكمة الابتدائية و محاكم الخدمة المدنية. "و الفرقة العاملة المعنية بالمادة 29 هي فريق عمل أوروبي مستقل يتعامل مع القضايا

---

[1] انظر نص المادة (83 الفقرتين 2-3) من اللائحة الاوربية لحماية البيانات الشخصة (GDPR)

[2]Reidenberg , J,R,OP,CIT,P ; 64.

المتعلقة بحماية الخصوصية والبيانات الشخصية. وقد تم إنشاؤه بموجب المادة 29 من التوجيه رقم 46 لسنة 1995 (توجيه "حماية البيانات") ونص عليها التوجيه رقم 58 لسنة 2002 (توجيه "الاتصالات الإلكترونية"). سلطات حماية البيانات في الدول الأعضاء في الاتحاد الأوروبي هي أعضاء في مجموعة العمل. بصرف النظر عنهم ، يشارك أيضًا المشرف الأوروبي على حماية البيانات وممثل المفوضية في أنشطة مجموعة العمل. تتمتع الدول الأعضاء في المنطقة الاقتصادية الأوروبية بوضع مراقب في هذه المجموعة ، فضلاً عن عدد من الدول الأعضاء المرشحة. قسم "حماية البيانات" في المديرية العامة للعدالة والحرية والأمن التابعة للمفوضية الأوروبية مسؤول عن إدارة مجموعة العمل والمهام الكتابية. و تصدر مجموعة عمل المادة 29 بانتظام الآراء وتنشر وثائق العمل والقرارات المتعلقة بحماية الخصوصية والبيانات الشخصية ، بهدف تطبيق منسق لهذه التوجيهات في الدول الأعضاء في الاتحاد الأوروبي. الفريق العامل المعني بالمادة 29 مسؤول أيضًا عن تقديم آراء الخبراء للمفوضية الأوروبية وبشأن مدونات السلوك على مستوى المجموعة.

المطلب الثاني

آلية التعامل بالبيانات الشخصية لزبائن الشركات المالية

أضحت البيانات الشخصية للأفراد محلا للتعامل فيما بين الجهات التي تقوم بجمعها وتصنيفها وحفظها والتعامل فيها ، وذلك بهدف الوصول إلى بيانات متكاملة عن كل فرد ، الا ان انتشار استخدام الانترنت في اغلب مجالات الحياة التي يتاح عبرها معلومات تخص الافراد المستخدمين لها يستلزم ان يكون هناك اطراف اساسية في هذه الالية اللازمة للتعامل في البيانات الشخصية لا تتم الا بها وهم المسؤول عن معالجة البيانات الشخصية (المراقب) والمعالج ، وصاحب البيانات ، اضافة الى اشخاص اخرين سنعرض لهم خلال البحث ، وهو ما سنتناوله في فرعين وكالاتي :

الفرع الاول

اطراف عملية التعامل بالبيانات الشخصية

لبيان كيفية التعامل بالبيانات الشخصية لابد من التعرف على اطراف هذه العملية القانونية ، وقد بينا في تعريف البيانات الشخصية كونها عائدة الى الشخص الطبيعي ، ومن ثم فأن الطرف الأول هو صاحب البيانات ونحيل لما تناولناه سابقا منعا للتكرار اما الطرف الثاني وهو الشركة وهذه الأخيرة تتعامل مع البيانات عن طريق عد\اة اشخاص نص عليها القانون وكالاتي :

اولا : المتحكم : عرفت اللائحة الأوروبية فتعرف "المتحكم controller " بأنه: (يعني الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تحدد، بمفردها أو بالاشتراك مع آخرين، أغراض ووسائل معالجة البيانات الشخصية؛ وعندما يتم تحديد أغراض ووسائل مثل هذه المعالجة بموجب

قانون الاتحاد أو الدول الأعضـاء، يجوز تحديد المتحكم أو المعايير المحددة لتحديده بموجب قانون الاتحاد أو قانون الدول الأعضاء) [1].

في حين عرف المشـرع المصـري "المتحكم في البيانات" بأنه (أي شـخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصـول علي البيانات الشـخصـية وتحديد طريقة وأسـلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقًا للغرض المحدد أو نشاطه)[2].

ويرى الباحث أن المشـرع المصـري قد اتبع نهج المشـرع الأوروبي في تحديد مفهوم المتحكم، حيث يعد المتحكم هو صـانع القرار الرئيسـي، ولديه السـيطرة على عملية جمع البيانات وعلى وسـائل وطريقة معالجتها[3]. وفي حالة وجود أكثر من متحكم في البيانات (المنظمات والمؤسسات عادةً) ، فيشكلوا وحدات تحكم مشـتركة تتشـارك المسـؤوليات والالتزامات القانونية كما تتشـارك تحديد الهدف من جمع البيانات والتحكم فيها. وقد أشـارت اللائحـة الأوروبيـة في المادة 26 منها لمسـألة التحكم المشـترك " Joint Controllers " بقولها إن: " 1- عندما يقوم اثنان أو أكثر من المتحكمين بشـكل مشـترك بتحديد أغراض ووسـائل المعالجة، فيجب أن يكونا متحكمين مشـتركين، وتحدد بطريقة شـفافة مسـؤوليات كل منهما عن الامتثال للالتزامات بموجب هذه اللائحة، خاصة فيما يتعلق بممارسة حقوق صاحب البيانات وواجبات كل منهما فى تقديم المعلومات المشار إليها في المادتين 13 و 14 ، عن طريق الوسائل وبالترتيب بينهما ما لم يتم تحديد مسـؤوليات كل متحكم بموجب قانون الاتحاد أو قانون الدول الأعضـاء الذي يخضـع له المتحكمون، وقد يقوم الترتيب بتخصيص نقطة اتصـال لأصـحاب البيانات. ويبدو أن القانون المصـري قد تعرض أيضًـا لفكرة التحكم المشـترك في (المادة 4 فقرة ثانية) من قانون حماية البيانات الشـخصـية التى نصـت على أن: "وفي حال وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصـوص عليها في

---

(1) انظر نص المادة 4 البند 7 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .

(2) انظر نص المادة الاولى من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

(3) عرف المشرع المصري المعالجة في المادة الاولى منه بانها (اي عملية الكترونية او تقنية لكتابة البيانات الشخصية ، او تجميعها ، او تسجيلها ، او حفظها ، او تخزينها ، او دمجها ، او عرضها ، او ارسالها ، او استقبالها ، او تداولها ، او نشرها ، او محوها ، او تغييرها ، او تعديلها ، او اسـترجاعها ، او تحليلها وذلك باسـتخدام اي وسـيط من الوسـائط او الاجهزة الالكترونية او التقنية سـواء تم ذلك جزئيا او كليا).في حين عرفت اللائحـة الاوربيـة ، وفى المادة 4 منها "المعالجة Processing " بأنها: (أي عملية أو مجموعة من العمليات التي يتم إجراؤها على البيانات الشـخصـية أو على مجموعات من البيانات الشـخصـية، سـواء بوسـائل آلية أم لا، مثل التجميع أو التسـجيل أو التنظيم أو الهيكلة أو التخزين أو التكييف أو التغيير أو الاسترجاع أو التشاور أو الاستخدام أو الإفصاح عن طريق الإرسال أو النشر أو الإتاحة أو المحاذاة أو الدمج أو التقييد أو المحو أو التدمير) .و تطرقت محكمة العدل الأوروبية فى العديد من أحكامها لتفسـير مصـطلح المعالجة وذكرت بعض الأعمال التى تعد من قبيل معالجة البيانات الشخصية، ولقد تطرقت لأول مرة لتفسير تعريف المعالجة عام 2003 فى قضية Lindqvist حين أوضحت أن نشر بيانات شخصية على صفحة إنترنت يعد من قبيل المعالجة التى تجعلها فى هذه الحالة مشمولة بالحماية التى يكفلها التوجيه الأوروبي رقم 46 /لسنة 1995. انظر

ECJ, Case C-101/01, 6th November 2003; [2003] ECR 1-12971), Found at: http // curia.europa.eu/juris/liste.jsf?num=C-101/01

كما صرحت المحكمة فى حكم شهير لها بأن أن تعديل أو تغيير Alternation البيانات الشخصية يعد فى حد ذاته من قبيل أعمال المعالجة، إلا أنه يمكن أن تنشـأ عمليات معالجة أخرى للبيانات دون أن يتم تعديلها. كما أشـارت المحكمة أن قدرة محرك البحث على "إتاحة" بيانات خاصـة بتاريخ وتفاصـيل البحث الذى قد يقوم به شـخص، تعد من قبيل المعالجة كما هو الحال بالنسبة لكل العمليات السابقة على الإتاحة مثل قيام محرك البحث بجمع وتسجيل وتنظيم وتخزين تلك البيانات بصورة تلقائية ومستمرة وممنهجة. انظر في ذلك:

Case-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE"), Paragrapghs 26-31.

هذا القانون، وللشـــخص المعنى ممارســـة حقوقه تجاه كل متحكم على حدة". ويتمثل معيار وجود تحكم مشـترك في تشـارك كيانين أو أكثر في تحديد أغراض ووسـائل عملية المعالجة، ويمكن أن يتجسـد التحكم المشترك فى شكل قرار مشترك يتخذه كيانان أو أكثر أو ينتج عن قرارات متقاربة من قبل كيانين أو أكثر، حيث تكون القرارات مكملة لبعضـها البعض وتكون ضـرورية للمعالجة، بحيث تتم بطريقة يكون لها تأثير ملموس على تحديد أغراض ووسـائل المعالجة. إضـافة إلى ضـرورة مشـاركة كلا الطرفين في المعالجة، وأن تشمل عملية التحكم المشترك على تحديد الأغراض من جهة وتحديد الوسائل من جهة أخرى [1] .

وعلى خلاف اللائحـة الأوروبيـة، التي تعرضـــت بـإيجـاز لوجوب تحـديـد المســـؤوليـة بين المتحكمين المشـتركين، لم يشر المشـرع المصـري لأي شروط خاصة بالتحكم المشترك ولم ينص على إمكانية تعيين نقطة اتصـال لتسـهيل الوصـول للمتحكم بدلاً من وضـع هذا العبء على الشـخص المعنى بالبيانات. ويمكن تفسـير هذا الاختلاف بين التشـريعات بأن المشـرع المصـري قد وضـع في قانون حماية البيانات ما يعتبره الحد الأدنى من الحماية المطلوبة وعليه فلا يســمح للأطراف بالاتفاق على تقســيم هذه الالتزامات أو نقل بعضــها إلى شــخص أخر، بل يجب أن يلتزم بها كل متحكم وذلك توفيرا لقدر أكبر من الحماية لصــاحب البيانات الذي يسـتطيع الرجوع على أيهما لترتيب المسـؤولية. ولكن لاتزال هناك اعتبارات عملية قد تثير إشــكاليات في ظل غياب تنظيم ومعايير للتحكم المشــترك. مثال ذلك تحديد مدى إمكانية أن يقرر أحد متحكمي البيانات إعادة استخدام البيانات لغرض جديد وهل توجد حاجة إلي أخذ موافقة المتحكم الآخر؟

ويخلص الباحث مما ســبق إلى اتفاق القانون المصــري مع اللائحة الأوروبية لحماية البيانات على أن المتحكم في البيانات هو الشخص الذي يحصل على البيانات بحسب طبيعة عمله وله الحق في تحديد طريقة وأسلوب الاحتفاظ بها ومعالجتها بشرط أن يكون ذلك في حدود الغرض المعلن والمحدد، الأمر الذي يحدده أيضاً المتحكم سواءً أكان متحكم واحد أو أكثر من متحكم مجتمعين.

ثانيا : المعالج :. هو الشخص القائم بمعالجة البيانات الشخصية ، وقد اطلقت عليه اللائحة الاوربية تسمية (المعالج) وعرفته المادة (4 البند 8) منها بأنه (الشخص الطبيعي او المعنوي او السلطة العامة او الوكالة او اي هيئة اخرى تقوم بمعالجة البيانات الشخصية نيابة عن المراقب) .

في حين عرف المشرع المصري المعالج في المادة الاولى من قانون حماية البيانات الشخصية رقم 151 لسـنة 2020 بأنه (أي شــخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشــخصــية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقا لتعليماته).

ويرى الباحث أنه ربما كان المشـرع المصـري في تعريفه للمعالج قد جانبه الصـواب وذلك لأنه لا داعي لذكر قابلية الشخص لمعالجة البيانات لصالح نفسه لأن ذلك يجعله متحكم.

في حين اطلقت عليه بعض التشـريعات تسمية "المناول" [2] ، وعرفته بانه (كل شخص طبيعي او معنوي يقوم بمعالجة المعطيات الشخصية لحساب المسؤول عن المعالجة)

---

[1] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Erpoian Data Protection Board Reoprt. 2020.

[2] ك قانون حماية البيانات الشخصية التونسي رقم 63 لسنة 2004 في الفصل السادس منه.

من خلال التعريفات السابقة يتضح ان القائم بمعالجة البيانات قد يكون شخصا طبيعيا او معنويا [1]، خاصا او عاما [2]، منفردا او مشتركا مع اخرين في معالجة البيانات لصالح المراقب.

وقد تطلبت بعض التشـــريعات [3]من المســـؤول عن معالجة البيانات في حالة اذا عهد ببعض اعمالها او جميعها الى الغير في اطـار تعـاقدي اتخـاذ كـافة الاحتياطات والتحري عند اختيار من يعهد اليه بذلك . كما يتعين على المعالج الا يتصـرف الا في حدود ما يأذن له به المسؤول عن المعالجة وان تكون لديه الوسائل الفنية اللازمة والملائمة لانجاز المهام المسندة اليه .

كما اشـارت اللائحة الاوربية الى انه في حالة اذا كانت معالجة البيانات تستند الى عقد ، فانه يصـبح ملزما للمعالج تجاه المراقب ، ويتعين ان يشـار في العقد موضـوع المعالجة ومدتها ، وطبيعتها والغرض منها ، ونوع البيانات الشـخصـية وتصـنيفاتها ، والالتزامات والحقوق ، كما يجب ان ينص فيه ايضـا على وجه الخصوص على ان المعالج ،لايعالج البيانات الشخصية الا بناء على تعليمات موثقة من المراقب ، بما ذلك نقل البيانات الى بلد ثالث او منظمة دولية مالم يقتض الامر ذلك بموجب قانون الاتحاد او قانون الدولة التي يخضـع له المعالج ، وان يضـمن الاشـخاص المأذون لهم بمعالجة البيانات قد التزموا بالسرية او يخضعون لالتزام قانوني ملزم بالسـرية ، واخيرا ضـرورة احترام الشـروط والبنود السـابقة في حالة اسـناد المعالجة لشخص اخر [4].

ويبدو من ذلك وجود قدر من الاختلاف الجزئي بين تعريف القانون المصـري وتعريف اللائحة الأوروبية بشـأن المعالج، حيث يجيز القانون المصـري للمعالج بأن يقوم "بعملية المعالجة" لصـالحه وليس لصـالح المتحكم، بينما يحصـــره تعريف اللائحة الأوروبية في قيامه بالمعالجة نيابة عن المتحكم. ويثور في هذا الشـأن التسـاؤل حول مسـؤولية المعالج في حالة قيامه بعملية المعالجة لصـالحه، وليس بناء على تعليمات المتحكم، وحول قصد المشرع المصري من إضافة إمكانية المعالجة لصالح المعالج.

ويرى الباحث في الاجابة على ذلك ، أنه في حالة قيام المتحكم بالمعالجة لصـالحه وليس لصـالح المعالج، فإنه هنا يقوم بدور المعالج وليس المتحكم.

وبوجه عام، يتفق كل من القانون المصـــري واللائحة الأوروبية على تحديد علاقة المتحكم والمعالج من خلال تحديد من له سـلطة اتخاذ القرار فيما يتعلق بمعالجة البيانات الشـخصـية، أي من له سـلطة تحديد غرض وطريقة المعالجة [5] .

وبناءً على ما سبق فإنه يجب ألا يقوم المعالج بمعالجة البيانات خلافًا لتعليمات المتحكم، وللمتحكم السلطة المطلقة في تعيين أطر وأغراض المعالجة بما يسـمح للمعالج باختيار أنسـب الوسـائل التقنية والتنظيمية

---

[1] كما هو الحال بشـأن بلدية كومو الايطالية حيث تقوم بمعالجة بيانات مسـتخدمي البوابة الالكترونية للبلدية للاسـتفادة من خدماتها والوصـول اليها ، حيث تقوم البلدية باعمال المعالجة اسـتنادا الى المرسـوم التشـريعي الايطالي رقم (198) لسـنة 2003 ، والمتعلق بحماية البيانات الشخصية للمزيد راجع الموقع الالكتروني للبلدية
http://www.comunc.como.it/il

[2] حيث اجازت بعض التشريعات للسلطة العامة ان تعالج البيانات المتعلقة بارقام السجل المدني بغرض تحديد الهوية بشكل لا لبس فيه او كأرقام ملفات ، انظر نص المادة (11) من قانون معالجة البيانات الشخصية لدولة جزر الفارو رقم 429 لسنة 2011.

[3] كالتشريع التونسي الخاص بحماية البيانات الشخصية لسنة 2004 على سبيل المثال في الفصل 20 منه .

[4] انظر نص المادة (28) الفقرة الثالثة من اللائحة الاوربية لحماية البيانات الشخصية .

[5]Rowenna Fielding, 'The Concept of Controller and Processor Data Entities' (2018

لخدمة الغرض الأســاســـي الذي يتم تجميع البيانات من أجله. ومع ذلك ووفقاً لكل من القانون المصـــري واللائحة العامة لحماية البيانات لا يجوز للمعالج مخالفة تعليمات المتحكم.

ثالثا : المعالج من الباطن :. في بعض الاحيان قد يعهد الشـخص القائم بمعالجة البيانات الشـخصـية القيام باعمال المعالجة كليا او جزئيا الى شـخص اخر يسـمى المعالج من الباطن (Ie sous – traitant) الذي عرفته بعض التشريعات [1] .

في حين عرفه المشرع الفرنسي بانه (كل شخص يقوم بمعالجة البيانات الشخصية لحساب المسؤول عن المعالجة يعتبر معالج من الباطن) [2] .

وبالرجوع الى التعاريف اعلاه يتضـح ان المعالج من الباطن هو كل شـخص سـواء كان طبيعيا او معنويا يقوم بمعالجة البيانات لحساب المسؤول عن المعالجة ، ويتعين ان يتضمن عقده مع المسؤول عن المعالجة التزامه بتوفير كافة الضـمانات اللازمة للحفاظ على سـلامة سـرية البيانات ، وان يتخذ جميع الاحتياطات اللازمـة للمحـافظة على امن البيانات ومنع الغير من تعديلها او الاضـــرار بها او الاطلاع عليها دون اذن صاحبها [3].

كما نصت اللائحة الاوربية (GDPR) على انه يجب على المعالج عدم اشراك اي معالج دون اذن كتابي مســبق محدد او عام من المراقب ، وفي حالة الحصـــول على اذن كتابي عام ، يتعين على المعالج القيام بابلاغ المراقب بأي تغييريات مقصودة تتعلق باضافة او استبدال المعالجات الاخرى ، مما يعطي المراقب فرصـــة الاعتراض على هذه التغييرات [4] . كما حظرت بعض التشـــريعات على المعالج من الباطن ان يعالج البيانات الشخصية دون اتباع تعليمات المسؤول عن المعالجة ، الا اذا اقتضت ذلك التزامات قانونية [5]. وفي جميع الاحوال يكون المعالج والمعالج من الباطن مســؤولين مدنيا عن كل اخلال بمقتضـــيات القانون [6] .

رابعا : الحائز :. استحدث القانون المصري مصطلح "الحائز" فى قانون حماية البيانات، والذى لم تتطرق إليه اللائحة الأوروبية. ولقد أكدت الجهة المعدة لمشروع القانون فى مذكرته الإيضاحية على ذلك بتوضيح أن وضـع الحائز هو وضـع قائم بالفعل وأنه سـوف يتلاشـى بعد فترة تسـتقيم فيها الأوضـاع . ولقد عرف القانون المصـــري الحائز بأنه: "أي شـــخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليا ببيانات شخصية في أي صورة من الصور، أو علي أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت

---

[1] اذ المادة الاولى (6) من قانون حماية الاشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي المغربي لعام 2009 بأنه (الشخص الذاتي او المعنوي او السلطة العامة او المصلحة او اي هيئة اخرى تعالج المعطيات ذات الطابع الشخصي لحساب المسؤول عن المعالجة).

[2] انظر نص المادة (35) من قانون المعلوماتية والحريات الفرنســي رقم (78) لســنة 1978 والمعدل باحكام القانون رقم (408) لسنة 2004 .

[3]Garance Mathias : Donnees personnelles : Votre conformite , Reglement europeen Donnees personnelles ,Loi pour une Republique Numerique, Loi de modernization de la jusice du XXIeme siècle , 16 FICHES PRATIQUES , Janvier 2017, Fiche n 9 : Le renforcement des obligations des sous – traitants

http://www.avocats-mathias.com/wp-personnel-Janvier-2017,pdf.

[4] المادة 28 من اللائحة الاوربية لحماية البيانات الشخصية

[5] نص المادة 25 من قانون حماية الاشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي المغربي لعام 2009.

[6] د. عبد الرحمن خليفة الرواس ،اثر التشريعات المتعلقة بحماية البيانات الشخصية على فعالية التجارة الالكترونية ، زين الحقوقية ، ط1 ، 2019، 133 .

إليه حيازتها بأي صورة".[1] وان انتقال البيانات الى الحائز اما ان تكون مباشرة من الزبون كما لو كانت هناك معاملة مالية بين الشركة والزبون تستوجب إعطاء البيانات للحائز (الشركة) او قد يكون حصوله على البيانات بطريقة أخرى كان يتم نقلها له من قبل الشركة المالية نتيجة معاملة لاحة يتم من خلالها تداول هذه البيانات . وجدير بالذكر أن مجلس الدولة كان قد علق على تعريف الحائز فى مشروع القانون مفضلاً ضبط صياغته بحذف عبارة "قانونياً أو فعلياً" وعلل ذلك بأن لفظ "يحتفظ" يشمل كافة أسباب حيازة البيانات الشخصية. كما أضاف مجلس الدولة أن حرف العطف (أو) يفيد المغايرة لغوياً بين كلاً من المعطوف والمعطوف عليه، وأن ذكر هذا الحرف بالتعريف يؤكد على أنه فى حالة احتفظ الشخص فعلياً بأي بيانات شخصية يعد من قبيل الحيازة غير المشروعة وفقاً لهذا التعريف مما يعد نتيجة غير منطقية لابد ألا يشملها مشروع هذا القانون[2] إلا أن رد قطاع التشريع بوزارة العدل جاء رافضًا لهذا المقترح وأجمعت اللجنة المعدة للمشروع على ضرورة الإشارة إلى كل من نوعي الحيازة، وذلك لإزالة أى غموض قد يلحق بالتعريف[3].

وإذا كان المشرع المصري قد انفرد بوضع تعريف خاص للحائز إلا أنه لم يفرض عليه أي التزامات خاصة به، بل اكتفى بالإشارة إليه في النصوص التي تنظم التزامات المتحكم والمعالج، ومع ذلك لم يخرج الحائز من إطار المحاسبة فنجد نصوصًا عقابية خاصة به في القانون، ومن هنا يثور التساؤل حول خصوصية مفهوم الحائز في القانون المصري، إذ لم نجد له مقابل على قدر اطلاعنا في القوانين المقارنة وخاصة اللائحة الأوروبية، وتزداد المسألة صعوبة إذا بحثنا عن طبيعة العلاقة بين الحائز و المعالج وهل هناك تداخل بين مفهوم الحائز ومفهوم المعالجة حيث أن كلاهما يدخل في إطار تعريفه الاحتفاظ بالبيانات الشخصية؟

للاجابة على ذلك يرى الباحث أن القانون لم يُلق على عاتق الحائز للبيانات الشخصية أية التزامات تذكر، وأن الحائز قد يكون أحد مندوبي التسويق أو المبيعات أو الشركات التي تعمل في هذا المجال حيث يمكن تداول مثل هذه البيانات بين العاملين في هذا المجال. وفى هذا الصدد نرى من الضروري، إما بوضع التزامات واضحة على كاهل الحائز أو الاستغناء عن تعريفه ضمن قائمة التعريفات التي أوردها القانون.

خامسا : المستفيد او المتلقي او المرسل اليه :. يعد المستفيد من التعامل بالبيانات الشخصية احد الاطراف في هذه العملية ، ويمكن القول بأن كل شخص طبيعي او معنوي يتلقى البيانات الشخصية [4] .

---

[1] انظر نص المادة الاولى من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[2] كتاب السيد المستشار/ نائب رئيس مجلس الدولة ورئيس قسم التشريع رقم (24) بتاريخ 16 يناير 2019 المرفق بتقرير اللجنة المشتركة بشأن "مشروع قانون بإصدار قانون حماية البيانات الشخصية"، تعديل تعريف الحائز، ص 108 .

[3] مذكرة قطاع التشريع بوزارة العدل بتاريخ 21 فبراير 2020 بالرد على ملاحظات قسم التشريع بمجلس الدولة رقم (24) بتاريخ 16 يناير 2019 المرفقة بتقرير اللجنة المشتركة بشأن "مشروع قانون بإصدار قانون حماية البيانات الشخصية"، رأى القطاع على تعديل تعريف الحائز، ص 125 .

[4]Voir CHAPITRE Ier Article 3 ,Loi n 78-17 du 6 janvier 1978 relative a I,informatique ,aux fichiers et aux libertes , Modifie par Loi n 2004- 801 du 6 aout 2004 : Le destinataire d,un traitement de donnees a caractere personnel est toute personne habilitee a reccvoir communication de ces donnees autre que la personne concernee le responsible du traitement , le sous-traitant.

وقد اطلقت عليه اللائحة الاوربية الملغاة تسمية المتلقي وعرفته بأنه (الشخص الطبيعي او الاعتباري او الهيأة العامة او الوكالة او اي هيأة اخرى يتم الافصاح لها عن البيانات ، ومع ذلك يجب الا ينظر الى السلطات التي قد تظهر البيانات في اطار تحقيق خاص كمتلقين)[1].

واطلقت عليه اللائحة الاوربية الحالية تسمية الطرف الثالث وعرفته بانه (شخصا طبيعيا او اعتباريا او سلطة عامة او وكالة او اي هيأة اخرى غير صاحب البيانات ، او المراقب او المعالج ، او الاشخاص الذين يحق لهم ، بموجب السلطة المباشرة للمراقب او المعالج ، معالجة البيانات الشخصية)[2] .

وبناء على ما سبق يمكن القول بأن المستفيد او المرسل اليه او متلقي البيانات ذات الطابع الشخصي هو الشخص الطبيعي او المعنوي او السلطة العامة او الهيأة ، و الذي يتلقى البيانات او الذي يستحصل على اذن بالاطلاع عليها ، ويختلف عن الشخص المعني بالمعالجة والمراقبة وعن المعالج وعن تابعي الاخيرين . وتطبيقا لذلك لايعد بمثابة مرسل اليه او مستفيد او متلقي للبيانات كافة السلطات المخولة قانونا طلب بيانات من المسؤول عن المعالجة .

سادسا : ضابط حماية البيانات :. جاءت اللائحة الاوربية لحماية البيانات الشخصية (GDPR) بشخص جديد يعد طرفا في عملية التعامل بالبيانات الشخصية ، حيث لم تشر له اللوائح والقوانين السابقة ، واطلقت عليه موظف او ضابط حماية البيانات ، والذي يتم تعيينه من قبل المراقب او المعالج اذا توافرت حالة من الحالات الاتية [3] :

1- اذا كانت عملية المعالجة تتم من قبل سلطة عامة او هيأة عامة بأستثناء المحاكم التي تتصرف بصفتها القضائية .
2- اذا كانت الانشطة الاساسية للمراقب او المعالج تتطلب بحكم طبيعتها ، نطاقها ، واغراضها رصد منظم ومنهجي لاصحاب البيانات وعلى نطاق واسع .
3- اذا كانت المعالجة تتم على نطاق واسع لفئة من الفئات الخاصة للبيانات ، او البيانات الشخصية المتعلقة بالادانات الجنائية والجرائم .

كما نصت على انه اذا كان المراقب او المعالج سلطة عامة او هيأة عامة فيجوز له تعيين ضابط حماية بيانات واحد للعديد من الجهات والهيئات مع مراعاة هيكلها التنظيمي وحجمها .

ويتم تعيين ضابط البيانات على اساس مؤهلاته المهنية ، لاسيما معرفته بقوانين وممارسات حماية البيانات والقدرة على الوفاء بالالتزامات المتعلقة بهذا العمل ، ويجوز ان يكون موظفا لدى المراقب او المعالج ، او ان يقوم بمهامه على اساس عقد خدمة ، ويلتزم المراقب او المعالج بنشر بيانات الاتصال الخاصة بهذا الموظف وابلاغها الى السلطة التي تتولى عملية الاشراف والرقابة على حماية البيانات الشخصية [4] .

ومن المهام التي يكلف بها ضابط حماية البيانات القيام بتقديم المشورة للمراقب او المعالج او الموظفين القائمين بمعالجة البيانات ، وكذلك القيام بتوعية وتدريب الموظفين المشاركين في التجهيزات والعمليات السابقة على المعالجة والتعامل ، وايضا تقديم المشورة عند الطلب فيما يتعلق بتقييم اثر حماية البيانات ،

---

[1] انظر نص المادة 4 من اللائحة الاوربية لحماية البيانات الشخصية رقم 46 لسنة 1995 الملغاة .
[2] انظر نص المادة 4 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .
[3] انظر نص المادة 37 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .
[4] انظر نص المادة 37 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .

واخيرا التعاون مع السلطة المختصة بالأشراف والرقابة على صور التعامل بالبيانات الشخصية من جمع وتصنيف ومعالجة وتداول البيانات [1] ، وهو ما سنتناوله في الفرع الثاني من هذا المطلب .

الفرع الثاني

مراحل التعامل بالبيانات الشخصية

تتنوع أساليب وصور التعامل في البيانات الشخصية للأشخاص، فأول صورة للتعامل في البيانات الشخصية هي تجميع البيانات " أي القيام بتجميع بيانات الأفراد من قبل الشركات الشركات ، وان تجميع البيانات الشخصية هي المرحلة الأولى من مراحل التعامل مع هذه البيانات . أما الصورة الثانية التي تكون بعد تجميع البيانات ، فهي تصنيفها ؛ وذلك لعمل ملف كامل لكل فرد بوضع البيانات التي تتعلق به في هذا الملف ، وذلك بجعل كل البيانات التي تم تجميعها في أوقات مختلفة عن الشخص نفسه في ملف منفرد . أما الصورة الثالثة فهي حفظ هذه البيانات في حافظات واقراص خاصة لمنع سرقتها واتلافها ، والصورة الاخيرة من صور التعامل بالبيانات الشخصية هي التعامل في البيانات الشخصية والاتجار بها ، حيث تقوم الشركات بالتعامل في البيانات الشخصية التي تم تجميعها وتصنيفها ، مع شركات وجهات أخرى بهدف الوصول إلى صورة متكاملة عن الشخص صاحب هذه البيانات ، بل ممكن الاتجار في البيانات الشخصية ، بحيث أصبحت البيانات الشخصية تشكل ثروة لكثير من الشركات التي تقوم باستثمارها و ببيعها لشركات أخرى [2]، وهذا ما سنتناوله تباعا وكالاتي .

اولا : جمع البيانات الشخصية [3] :. ادى التقدم التكنولوجي الى تطور واضح داخل المؤسسات التجارية والادارية ، مما انعكس ذلك على تحويل الدعامات الورقية الى ملفات الكترونية بواسطة استخدام الحاسب الالي بتلك المنشأة او الشركة . وبناء عليه فأضحى تجميع البيانات الشخصية بواسطة الدعامات الالكترونية بكل يسر ويتم حفظها داخل حواسيب مرتبطة بالانترنت ، الامر الذي يثير القلق فيما يخص مصير هذه البيانات ، هل ستنتهك خصوصيتها ام ستتم حمايتها[4] ؟.

واكثر مايثير القلق حاليا بخصوص البيانات الشخصية هو وجود شركات تعمل على تجميع اكبر قدر ممكن من البيانات من اجل تسويقها لاكبر الشركات التي تستخدم بدورها هذه البيانات من اجل تحقيق مبيعات ضخمة .

وتستخدم العديد من الوسائل التقنية لمحاولة تتبع البيانات الشخصية للزبائن وتجميعها، من ابرزها :

---

[1] انظر نص المادة 39 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .

[2] د. كريم محمد محي الدين سليم ، مصدر سابق ، ص 306 .

[3] د. عمرو طه بدوي ، التنظيم القانوني لمعالجة البيانات الشخصية ، ط1، دار النهضة العربية ، القاهرة ، 2020 ، ص63 .

[4] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، القسم الاول ، مصدر سابق ، ص419 .

1- جمع المعلومات الشخصية عن طريق استخدام تقنيات الانترنت :. تقدم هذه البيانات عن طريق الشخص نفسه ، اذ انه من المعروف ان غالبية مواقع الانترنت تطلب معلومات محددة من المستخدم قبل دخوله الموقع الخاص بالشركة ، فمواقع التسوق ومواقع البريد الالكتروني ومواقع التواصل الاجتماعي وشركات الصيرفة و التحويل المالي وغيرها تطلب من الشخص في الاغلب ذكر الاسم واللقب والعمر والعنوان والمستوى العلمي والحالة الاجتماعية وغيرها ، وايضا رقم البطاقة الائتمانية كما في مواقع التسوق[1].

وقد يتم جمع هذه البيانات تلقائيا عند الدخول الى موقع الشركة ، مثل عنوان الكمبيوتر الخاص بالزبون (IP) ، لان كل جهاز كمبيوتر متصل بالانترنت يمنح عنوان متكون من 32 رقما ، وكذلك البيانات الخاصة بالزبون ووقت زيارة الموقع وغيرها، وسواء فيما اذا كانت تلك البيانات تم اخذها من المستخدم او بشكل تلقائي في حال دخوله للمواقع المختلفة.

2- تقنيات الكوكيز (COOKIES) الكوكيز هي (عبارة عن ملفات نصية بأمتداد (TXT) يرسلها الخادم الخاص بالمواقع التي يتم زيارتها عبر الانترنت ، الى القرص الصلب للكمبيوتر الخاص بالمستخدم ، ويحتفظ بنسخة لديه ، وتحتوي على بيانات شخصية تخص المستخدم او الزبون وجهاز الحاسوب الخاص به ايضا ، كطريقة الاتصال بالشركة ، وعنوان الانترنت (IP) والشركة التي تمت زيارتها ، ونوع الجهاز والمعالج ، وايضا المعلومات التي يتطلب ادخالها من الزبون لاستمارة التسجيل ، مثل الاسم ورقم البطاقة الائتمانية ، والبريد الالكتروني ، والعنوان ، وغيرها) [2]، وتحتفظ الشركات التي تتم زيارتها بنسخة من ملفات الكوكيز داخل السيرفرات الخاصة بها ، شاملة للمعلومات السابقة ، وتستخدم تقنية الكوكيز للتعرف على الزبون في حال زيارته موقع الشركة مرة ثانية ، وذلك من اجل تسهيل الوصول للموقع الالكتروني الخاص بالشركة ، فاذا ما كان يستخدم معلومات معينة للدخول لهذا الموقع فلا يتطلب ادخالها مرة ثانية اضافة الى سرعة الدخول للموقع ، ولكن يبدو ان هناك خطورة في حال وجود هذه البيانات على جهاز الزبون ، اذ تستطيع الشركة من خلال الموقع الالكتروني الخاص بها ان تتعرف بسهولة على اتجاهات وخطوات الزبون عبر الانترنت ، من خلال المواقع التي يدخلها ، وهو الامر الذي يمكن ان يتم استخدامه للاعلانات [3]، اذ ان معرفة سلوك الزبون يحدد في النهاية الاشياء التي يحبها والاشياء التي يكرهها ، مما يعني ان من السهولة على المواقع الاعلانية توجيه اعلانتها التي تناسب ذوق الزبون ، هذا من جانب ومن جانب اخر فأنه يمكن سرقة هذه الملفات من جهاز الكمبيوتر الخاص بالزبون ، واستخدام البيانات التي يضمها ملف الكوكيز في التصفح بدلا عنه ، مما يعني انه قد يسهل اختراق الموقع الالكترونية والصفحات الشخصية والبريد الالكتروني الخاصة بالزبون، وايضا تكون هناك خطورة فيما اذا تم الاستيلاء على الكوكيز الخاص بالشركة ، اذ يعني اختراق ذات الموقع ، من خلال استخدام البيانات الموجودة داخل ملف الكوكيز .ونظرا لهذه الخطورة اشترط المشرع المصري شروطا لجمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل، صدور موافقة صريحة من الشخص المعنى بالبيانات أو فى الأحوال المصرح بها قانونا. كما اشترط لجمع البيانات ومعالجتها والاحتفاظ بها، ضرورة توافر أربعة شروط، هي:

---

[1] انظر د. يونس عرب ، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي ، دراسة منشورة على الانترنت http://www.arablaw.org .

[2] د. باسم محمد فاضل مدبولي ، مصدر سابق ، ص 58 .

[3] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، مصدر سابق ، ص 415 .

1- أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعنى.
2- أن تكون صحيحة وسليمة ومؤمنة.
3- وأن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.
4- ألا يتم الاحتفاظ بها لمدة أطول من المدة الزمنية اللازمة للوفاء بالغرض المحدد لها .

ويلاحظ أن المشرع المصري أشار إلي هذه المسائل باعتبارها شروط للجمع والمعالجة، بينما نجد اللائحة الأوروبية تشير إليها فى الفصل الثانى منها، الخاص بالمبادئ، باعتبارها المبادئ المتعلقة بمعالجة البيانات الشخصية والتي تتمثل فى المشروعية والشفافية وتحديد الغرض الصريح والواضح والمشروع واشتراط الملاءمة والصلة للأغراض التي تم تجميع البيانات من أجلها[1]. وفي كل الأحوال يجب ان يتحقق رضا الشخص المعنى بالبيانات ، ولبيان كيفية الحصول على الرضا يجب التطرق الى عدة نقاط وهي :

- وجود الرضا: يعد الرضا الصريح للشخص المعني بالبيانات شرطاً أساسياً لمشروعية كافة العمليات التى تتم على البيانات الشخصية، سواء جمع البيانات أو معالجتها أو الإفصاح عنها أو إفشائها، ما لم يصرح القانون بغير ذلك. ومن ثم يجب لتوافر رضا الشخص وجود الإرادة وأن يعبر عنها بصورة صريحة جازمة تُعبر عن موافقته على العمليات المزمع القيام بها على بياناته. ومن ثم لا يعتد بالتعبير الضمني عن الموافقة أو المعلقة على شرط، وبهذا تعد موافقة الشخص هي الأساس القانوني للمعالجة، ومرجع ذلك إلى أن بياناته تمس خصوصيته وقد تمتد إلى حياته العائلية التى يحرص أن تكون بعيدة عن الأنظار.

وقد تطلب المشرع المصري صراحة فى المادة الثانية وجود الرضا الصريح للشخص على جمع ومعالجة البيانات، وهو عين ما أخذت به اللائحة الأوروبية فى المادة 6 منها، كما حددت المادة 7 من اللائحة شروط الموافقة . وقد عرفت المادة 4/ 11 من اللائحة الأوروبية "موافقة" صاحب البيانات " بأنها تعني (أي إشارة صريحة ومحددة وواضحة لا لبس فيها، تدل على رضا صاحب البيانات والتي يشير من خلالها إلى الموافقة على معالجة البيانات الشخصية المتعلقة به أو بها، من خلال بيان أو بعمل إيجابي واضح). بينما أغفل المشرع المصري تعريف "موافقة الشخص المعنى بالبيانات" على جمع ومعالجة البيانات، على عكس المشرع الأوروبي .

ويرى الباحث انه من الضروري تحديد الموافقة وأن تذكر شروط ومعايير واضحة لهذه الموافقة، فى مادة مستقلة، وتحدد شكل هذه الموافقة، سواء أكانت كتابية أو مجرد علامة على خانة فى موقع إلكتروني، حتى تأتي الموافقة مستنيرة ومبنية على فهم وإرادة حقيقية، ويضاف إلى ذلك موافقة من ينوب عن الشخص المعنى متى كان عديم الأهلية أو ناقصها.

- شكل موافقة الشخص المعنى:

---

[1] تجدر الإشارة إلى أن الحماية القانونية للبيانات الشخصية في فرنسا، وفقًا للفصل الثاني من قانون) 18 - 1978 (والمعدل وفقًا للتعديات بموجب القانون رقم) 2004-701 الصادر فى 6 أغسطس 2004 قد نصت على شروط معينة لضمان مشروعية جمع ومعالجة البيانات الشخصية، وهي كما يلي (م 8)

1- عدالة ومشروعية طريقة جمع ومعالجة البيانات الشخصية.

2- وضوح وتحديد أهداف وأغراض جمع المعلومات، وأن يكون هناك توافق بين طريقة جمع المعلومات وغرض جمعها.

3- أن تكون طريقة جمع المعلومات كافية ومناسبة وذات صلة بالقياس للغرض الذي تم من أجله جمعها ومعالجتها. لمزيد من التفصيل فى هذا الخصوص، راجع: د. وليد السيد سليم: ضمانات الخصوصية في الانترنت، دار الجامعة الجديدة، الإسكندرية ، 2012 ، ص 588 .

هناك مفارقة مصدرها نصوص القانون، فقد غاير المشرع المصري فى الشكل الذى يجب أن تفرغ فيه الموافقة، فمن ناحية تطلبت فى حالة البيانات الشخصية، صدور موافقة صريحة من الشخص المعنى بالبيانات [1]، بينما فى حالة البيانات الشخصية الحساسة، الحصول على موافقة كتابية صريحة من الشخص المعنى، وهو ما يكون على الشكل التالي[2]:

البيانات الشخصية: موافقة صريحة

البيانات الشخصية الحساسة: موافقة كتابية صريحة وهو ما يقطع بما لايدع مجالا للشك حول استلزام الكتابة عند صدور الموافقة على معالجة وجمع البيانات الشخصية الحساسة.

ولكن يظل التساؤل مُثاراً عن الصورة التى تُفرغ فيها الموافقة الصريحة التى تطلبها القانون المصري في حالة البيانات الشخصية (غير الحساسة)، فالقانون لم يستلزم أن تتخذ هذه الموافقة طريقاً معيناً أو شكلاً مخصوصاً، ومن ثم يكون للشخص وفقاً للقواعد العامة حرية كاملة فى التعبير عن الموافقة على الوجه الذى يراه، فالتعبير يكون صريحاً إذا قصد به صاحبه إحاطة الغير علماً بإرادته، أياً كان المظهر الذي يتخذه، شفاهة أو بالكتابة، أياً كانت عباراتها أو صورتها، سواء بصورة شخصية، كخطاب أو برقية، أو بصفة غير شخصية، كإعلان أو نشرة، أو بالإشارة التى لها دلالة بين الناس[3].

ونعتقد أنه رغم عدم اشتراط المشرع إفراغ الموافقة في شكل مكتوب، إلا أن الشخص المسؤول، المتحكم أو المعالج، سيكون حريصاً على الحصول عليها في صورة مكتوبة لضمان نسبتها لصاحبها وتيسيراً لإثباتها، وغالباً ما يتم إعداد نماذج محددة لإفراغ هذه الموافقة وفق الضوابط التي يتطلبها القانون.

- صحة رضا الشخص المعني بالبيانات: لا يكفي مجرد وجود رضا الشخص المعني بالبيانات، إنما يجب فوق ذلك أن يكون صحيحاً، وهو يكون كذلك متى وجدت الإرادة، فإذا انعدمت الإرادة انعدم الرضا، واستحال توافره نتيجة لانعدامه [4]، وعلى ذلك لا يتوافر الرضا إلا إذا توافرت الأهلية لدى الشخص المعني بالبيانات، والأهلية المطلوبة هنا هي أهلية الأداء أي صلاحية الشخص لاستعمال الحق ، أو بمعنى آخر قدرة الشخص على أداء التصرفات القانونية لحساب نفسه، ومناطها التمييز أو الرشد، إذ تتأثر بالسن والعقل، فيجب أن يصدر التعبير من شخص اكتملت مداركه ونضجت، فأصبح يقدر الآثار المترتبة على تصرفاته.

وباستقراء نصوص القانون نجدها تخلو من اشتراط أن يكون الشخص المعنى بالبيانات بالغاً سن الرشد ، أو تحديد سن معين، وهو في اعتقادنا شرط بديهي لخطورة الآثار القانونية المترتبة على عمليات معالجة البيانات وهو ما يتطلب اكتمال إدراك الشخص حتى يتبين تصرفاته.

وفى هذا الصدد تنص المادة 45 مدني مصري على أن: لا يكون أهلاً لمباشرة حقوقه المدنية من كان فاقد التمييز لصغر فى السن أو عته أو جنون. وكل من لم يبلغ السابعة يعتبر فاقداً للتمييز.

كما تنص المادة 46 من القانون المدني المصري رقم 131 لسنة 1948 على أن: "كل من بلغ سن التمييز ولم يبلغ سن الرشد، وكل من بلغ سن الرشد وكان سفيها أو ذا غفلة، يكون ناقص الأهلية وفقاً لما يقرره

---

[1] انظر نص المادة 2 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020

[2] انظر نص المادة 12 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

[3] انظر نص المادة(1/80) من القانون المدني العراقي رقم 40 لسنة 1950 والمقابلة لنص المادة (1/9) من القانون المدني المصري رقم 151 لسنة 1948 .

[4] د.مصطفى الجمال ، د. رمضان ابو السعود ، د. نبيل ابراهيم سعد ، مصادر واحكام الالتزام ، منشورات الحلبي ، بيروت ، 2003 ، ص50 .

القانون". ومن ثم لا يتوافر الرضا إذا صدر عن شخص غير مميز، كالمجنون والمعتوه، والصغير دون السابعة، وفاقد الوعي لسبب عارض، كمرض أو سُكر أو تخدير أو تنويم، لأن هؤلاء معدومي الإرادة . كذلك لا تصح الموافقة إذا صدرت ممن لم يبلغ سن الرشد أو بلغه ولكن كان مصاباً بسفه أو غفلة.

وحيث تنص المادة 47 من القانون المدني المصري رقم 131 لسنة 1948 على أن: "يخضع فاقدو الأهلية وناقصوها بحسب الأحوال لأحكام الولاية أو الوصاية أو القوامة بالشروط ووفقاً للقواعد المقررة فى القانون".

ومن ثم يجب موافقة الشخص على عمليات المعالجة، متى كان بالغاً سن الرشد، أما فى حالة عدم بلوغه، أو كان بالغاً ومصاباً بعاهة عقلية، فيجب الحصول على موافقة من ينوب عنه قانوناً (كالولي أو الوصى) ومن الغريب أن المشرع استلزم موافقة "ولي الأمر" فى حالة إجراء أى عملية جمع أو معالجة أو غيره على البيانات الشخصية الحساسة التى تتعلق ببيانات الأطفال.

وكان يُفضل لو قام المشرع المصري بتحديد سن محدد للرضا في اطار البيانات الشخصية ، كما فعلت اللائحة الأوروبية، فى المادة 8 منها، حيث اعتبرت معالجة بيانات الطفل فى إطار خدمات مجتمع المعلومات مشروعة، حين يكون سن الطفل 16 عاماً على الأقل، أما إذا كان سنه لا يتجاوز ذلك، فإن المعالجة لا تكون مشروعة، إلا إذا صدر الرضا من قبل صاحب السلطة الأبوية على الطفل (من ينوب عنه قانوناً). ويجوز للدول الأعضاء تخفيض هذا السن بشرط ألا يقل بأى حال من الأحوال عن 13 سنة [1].

- الموافقة الصريحة على حركة البيانات الشخصية عبر الحدود حال عدم توافر مستوى الحماية المطلوب:

تشترط المادة 15 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 عند نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية المنصوص عليه في القانون، ضرورة الحصول على الموافقة الصريحة للشخص المعني أو من ينوب عنه، وذلك فى الحالات الآتية:

1- المحافظة على حياة الشخص المعني بالبيانات، وتوفير الرعاية الطبية أو العلاج أو إدارة الخدمات الصحية له.
2- تنفيذ التزامات بما يضمن إثبات حق أو ممارسته أمام جهات العدالة أو الدفاع عنه.
3- إبرام عقد، أو تنفيذ عقد مبرم بالفعل، أو سيتم إبرامه بين المسئول عن المعالجة والغير، وذلك لمصلحة الشخص المعنى بالبيانات.
4- تنفيذ إجراء خاص بتعاون قضائي دولي.
5- وجود ضرورة أو إلزام قانوني لحماية المصلحة العامة.
6- إجراء تحويلات نقدية إلى دولة أخرى وفقاً لتشريعاتها المحددة والسارية.
7- إذا كان النقل أو التداول يتم تنفيذاً لاتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفاً فيه.

- اشتراط موافقة الشخص المعنى على التسويق الإلكتروني المباشر له:

تحظر المادة 17 من قانون حماية البيانات الشخصية المصري إجراء أى اتصال إلكتروني بغرض التسويق المباشر للشخص المعنى بالبيانات إلا بعد الحصول على موافقة منه، إلى جانب توافر الشروط

[1] انظر نص المادة (8/ 1) من اللائحة الاوربية لحماية البيانات الشخصية .

الأخرى التي يتطلبها نص المادة ومنها وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها. ويلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها أو عدم اعتراضه على استمراره ، بشأن تلقى الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال [1].

ثانيا : تصنيف البيانات :. بعد ان يتم تجميع البيانات الشخصية من خلال الشركات او المؤسسات كما مر ذكره ، فيتم الانتقال للمرحلة الثانية وهي تصنيف البيانات الشخصية ، ويعني تخصيص ملف لكل زبون يتضمن جميع البيانات الشخصية الخاصة به حتى تساعدها في عملية " التسويق المباشر "[2] .

بيد ان الشركات المتخصصة بتجميع هذه البيانات تعمل على ان يكون هناك اكثر من تصنيف داخل الملف ، فمثلا يكون الملف الشخصي الخاص بالزبون يحتوي على بيانات عديدة كالمهنة والاسم والايميل ورقم التليفون والحالة الاجتماعية والحالة الصحية ، اذ يكون التصنيف داخل الملفات الى بيانات عامة ، وبيانات تتعلق بحالته الصحية وبيانات تتعلق بحالته الاجتماعية[3] .

و الهدف من ذلك هو الاستفادة من البيانات بأفضل ما يمكن ، حيث تساعد هذه الطريقة على تنظيم عروض دعائية لكل زبون ، فمثلا البيانات التي تشمل المهنة والاسم والايميل ورقم التليفون تسوقها الى محلات الازياء لعرض البضائع على الزبائن من خلال ارسال رسائل على الايميل او التليفون والواتس اب ، اما البيانات المتعلقة بحالته الصحية تقوم بتسويقها للمستشفيات الخاصة .

وكانت هناك صعوبة في الماضي ، اذ كان يتم استخدام الكمبيوتر لصنيف كميات كبيرة من البيانات الشخصية ، لكن اختلف الامر حاليا فهناك برامج صممت لتساعد على اجراء تصنيفات مختلفة بكل سهولة ودقة .

اذ ان تصنيف البيانات الشخصية يعتمد على تقنيات وبرامج الكمبيوتر التي تستطيع تصنيف البيانات وفرزها والربط بينها ، بحيث يتم يكون هناك ملف متكامل عن الشخص ، يضم كل البيانات المتاحة عن الزبون ، ويكون ذلك دون تدخل بشري ، اذ يكفي ان يقوم الشخص بادخال بيانات الزبائن للكمبيوتر، حتى يقوم الكميوتر بتصنيفها ووضعها في الملف الخاص بالزبون [4].

وعليه فانه عندما يقوم الزبون بالاتصال هاتفيا باحد الشركات او مكاتب التحويل المالي ، فأن هذا المكتبر لا يطلب منه هنا بيانات عن الاسم او العنوان الذي سيرسل الي المبالغ ، لان كل البيانات الخاصة بالزبون تكون محفوظة ومصنفة عند الشركة او المكتب ، اذ توجد عنه قاعدة بيانات متكاملة عن هذ الزبون[5] .

---

[1] انظر نص المادة 18 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[2] د. باسم محمد فاضل مدبولي ، مصدر سابق ، ص 61 .

[3] د/ عبد الرحمن جمال الدين حمزة، الحق في الخصوصية في مواجهة حرية الإعلام ، اطروحة دكتوراه، كلية الحقوق، جامعة المنوفية، 2002 ، ص 339 .

[4] Sulliman Omarjee , Le data mining : Aspects juridiques de I,intelligence artificielle au regard de la protection des donnees personnelles , memoire , faculte de droit , universite montpellier I, Annee universitaire 2001-2002 , et disponible sur www/droitntic.com , p 13.

[5] OMARJEE,op-citp,p15

وفي اغلب الاحيان لاتعتمد الشـــركة على المعلومات التي قامت بجعها فقط ، بل انها تكمل هذا المعلومات بمعلومات اخرى تم تجميعها من قبل شـركات اخرى ، وهذا ما يؤدي الى التعامل في البيانات الشـخصـية والاتجار بها[1] .

علما ان المشرع المصري واللائحة الاوربية اشترطا لصحة تصنيف البيانات الشخصية الشروط نفسها الخاصة بجمعها والتي تم ذكرها في النقطة ثانيا من هذا الفرع .

ثالثا : حفظ البيانات الشخصية :. تتأثر مدة حفظ البيانات الشخصية مباشرة بالهدف المرجو من البيانات الشخصية ، كما تتأثر بمبدأ الملائمة ، الذي يفرض جمع المعلومات الضرورة ، واللازمة فقط .

وعليه لايمكن الاحتفاظ بالبيانات الشخصية لفترة غير محددة ، اذ يفترض ان تحدد المدة على اساس طبيعة البيانات ، والهدف من حفظها ومعالجتها ، بحيث يتم اتلافها او محوها ا ارشفتها او تشفيرها ، عند تحققه ، اذ تختلف مدة الاحتفاظ بالبيانات الخاصة بالموظفين عن تلك التي تجمع عن الزبائن .

بيد ان البيانات الشـخصـية تشـكل خطرا حقيقيا في حالة الاحتفاظ بها بدون ضـوابط ، اذ حظر المشـرع المصري الاحتفاظ بالبيانات التي يتم معالجتها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.[2] فالاحتفاظ بالبيانات لا يجوز أن يكون أبدياً بل يكون مؤقتاً ومحدداً لمدة معينة، ويعنى ذلك أنه يتعين على المعالج أن يقوم بحفظ البيانات التي تمت معالجتها لمدة زمنية معينة بحيث لا تتجاوز المدة المطلوبة للأغراض التي جمعت من أجلها)[3]

وتأكيداً على هذا الشـرط اتجهت اللائحة الاوروبية، في المادة 5 بند هـــ ، إلى ضـرورة أن يتم معالجة البيانات في شكل يسمح بتحديد هوية صاحب البيانات لمدة معينة، لا تزيد عما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها. ومع ذلك أجازت المادة نفسها (بند هـــ)، لأغراض معالجة البيانات الشخصية، تخزين البيانات الشخصية لفترات أطول، لأغراض الأرشفة من أجل المصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصـــائية، مع مراعاة التنفيذ الفني والتنظيمي المناسب واتخاذ التدابير المطلوبة للحفاظ على حقوق وحريات صاحب البيانات.

ورغم أهمية شرط الاحتفاظ بالبيانات الشخصية لمدة معينة، إلا أنه لا يوجد ضابط لتحديد هذه المدة. ولهذا يقع على عاتق اللائحة التنفيذية وضع الضوابط اللازمة لذلك. كذلك لم يقرر المشرع المصري عقوبة في حالة اذا ما تم الاحتفاظ بالبيانات الشخصية لمدة تزيد عن المدة اللازمة للوفاء بالغرض المحدد لها.

اذ انه وكما تم ذكره يجب ان تجمع البيانات لغرض واضـــح ومحدد ومشـــروع ، فيجب على القائم بعملية المعالجة ان يقوم بحفظ هذه البيانات لمدة لا تزيد عما هو ضـــروري لتحقيق الغاية من جمع هذه البيانات ، اذ ان هذه المدة تكون متوقفة على الغرض من جمع هذه البيانات [4].

---

[1] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، القسم الاول ، مصدر سابق ، ص399.

[2] انظر نص المادة الثالثة الفقرة (4) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[3] د. عمرو طه بدوي ، مرجع سابق ، ص 103 .

[4] Alexandare Menais and Sophie des Courits , High standards apply to personal data processing , Art on line at www . juriscom . net .

وعلى هذا يجب على المسؤول على جمع البيانات الشخصية ان يقوم بشكل دوري ومستمر بمراجعة البيانات التي تم خزنها ويقوم بحذف كل البيانات التي تم تحقيق الهدف من جمعها[1].

رابعا : التعامل في البيانات الشخصية والاتجار بها :. أصبحت البيانات الشخصية للأفراد محلا للتعامل بين الجهات التي تقوم بجمعها" فكل شركة تقوم بتبادل البيانات التي جمعتها مع شركات أخرى " وذلك بهدف الوصول إلى بيانات متكاملة عن كل فرد[2] .

ونقل هذه البيانات أصبح سهلا الآن مع استخدام الشبكات ، حيث يتم تكوين شبكة بين الحاسبات التي تتضمن قواعد بيانات لعدة جهات ، فيكون انتقال هذه البيانات بين تلك الحاسبات سهلا جدا، ودون حاجة لتدخل بشري ، بل إن الأخطر من ذلك، أن البيانات الشخصية أصبحت اليوم محلا لاقتصاد جديد، ومحلا للاتجار بها من قبل الجهات التي تقوم بجمعها، وتجلب المال لهذه الجهات . فسهولة جمع البيانات الشخصية ومعالجتها وانخفاض تكاليفها أدى إلى قيام كثير من المنشآت التجارية إلى التخصص في جمع وبيع هذه البيانات الشخصية إلى الجهات التي تريدها، بل إن هناك كثيرا من الشركات التي قامت ببيع البيانات الشخصية التي كانت في حوزتها بعد إفلاسها وتصفيتها وخروجها من السوق .

وتحظر المادة 17 من قانون حماية البيانات المصري إجراء أى اتصال إلكتروني بغرض التسويق المباشر للشخص المعني بالبيانات إلا بعد الحصول على موافقة منه، إلى جانب توافر الشروط الأخرى التي يتطلبها نص المادة ومنها وضع آليات واضحة وميسرة لتمكين الشخص المعني بالبيانات من رفض الاتصال الإلكتروني أو العدول عن موافقته على إرسالها. ويلتزم المرسل لأي اتصال إلكتروني بغرض التسويق المباشر الاحتفاظ بسجلات إلكترونية مثبت بها موافقة الشخص المعني بالبيانات وتعديلاتها أو عدم اعتراضه على استمراره، بشأن تلقي الاتصال الإلكتروني التسويقي وذلك لمدة ثلاث سنوات من تاريخ آخر إرسال .

و من القواعد الأساسية في لائحة حماية البيانات في الاتحاد الأوروبي أن نقل البيانات الشخصية خارج الاتحاد الأوروبي محظور الا اذا تحققت شروط معينة شروط معينة. سبب هذا التقييد هو الخوف من فقدان مواقف حماية البيانات في البلد الذي يتم نقل البيانات اليه. اذ يضمن البلد الثالث المعني مستوى مناسبًا من الحماية. بحيث يجب أن تؤخذ في الاعتبار مدى كفاية مستوى الحماية الممنوحة من قبل الدولة التي يتم نقل البيانات اليها في ضوء جميع الظروف المحيطة بعملية نقل البيانات أو مجموعة عمليات نقل البيانات ؛ يجب إيلاء اعتبار خاص لطبيعة البيانات والغرض وعملية المعالجة المقترحة أو العمليات ، بلد المنشأ وبلد المقصد النهائي ، قواعد القانون ، العامة والقطاعية ، السارية في البلد المعني والقواعد المهنية والإجراءات الأمنية التي يتم الالتزام بها في تلك الدولة.

وفي مصر، فقد حظر المشرع، بموجب الفقرة الأولى من المادة (21) من قانون حماية البيانات الشخصية المصري، (إجراء عمليات نقل للبيانات الشخصية التي تمّ جمعها أو تجهيزها للمعالجة إلى دولة أجنبية أو تخزينها أو مشاركتها إلّا بتوافر مستوى من الحماية في هذه الدولة لا يقلّ عن المستوى المنصوص عليه في القانون المذكور، وبترخيص أو تصريح من المركز). كما أوضحت الفقرة الثانية من المادة ذاتها أن (اللائحة التنفيذية لقانون حماية البيانات الشخصية تحدّ د السياسات والمعايير والضوابط والقواعد اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود وحمايتها).

---

[1]Cristina Cotaneu , the cyberconsumer, protection ,on, line at : www.droit-technologie.org,the data of being on line is , 2001,p11.

[2]د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، مصدر سابق، ص403.

ومع ذلك، فقد أورد المشرع المصري في المادة (22) من قانون حماية البيانات الشخصية المصري عدة استثناءات من حكم المادة (21) سالفة الذكر، (سمح فيها بنقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية المنصوص عليه في المادة (21)، وهو ما بينها سابقا في الاطروحة .

هذا، وقد جاءت الفقرة الأولى من المادة (23) من قانون حماية البيانات الشخصية المصري بحكم خاص مفاده "جواز قيام المتحكم أو المعالج، بحسب الأحوال، بإتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج جمهورية مصر العربية بترخيص من المركز، متى توافرت الشروط الآتية:

1- اتفاق طبيعة عمل كل من المتحكمين أو المعالجين، أو وحدة الغرض الذي يحصلان بموجبه على البيانات الشخصية.
2- توافر المصلحة المشروعة لدى كل من المتحكمين أو المعالجين للبيانات الشخصية أو لدى الشخص المعني بالبيانات.
3- ألا يقل مستوى الحماية القانونية والتقنية للبيانات الشخصية لدى المتحكم أو المعالج الموجودة بالخارج عن المستوى المت وافر في جمهورية مصر العربية".

كما أشارت الفقرة الثانية من المادة ذاتها إلى أن "اللائحة التنفيذية لقانون حماية البيانات الشخصية هي التي تحدد الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لذلك".

وممكن ان تستثمر هذه البيانات في الجانب التجاري اذ تعد البيانات الشخصية مجال اقتصادي مهم للقائمين على الدعائية عبر الانترنت ، اذ ان بيع الشركة بيانات الزبائن الذين يتعاملون معها و يترددون على موقعها الى شركات الاعلان باعداد قواعد بيانات تحدد من خلالها احتياجات الزبائن واذواقهم .

اذ ان الزبون عند دخوله الى هذه المواقع الالكترونية وبالتحديد الشركات المالية موضوع البحث يدلي ببياناته من اجل الاشتراك واجراء المعاملات اللازمة ، والواقع ان الشخص يدلي ببياناته بموافقته ، ولكن ممكن ان تستعمل هذه البيانات دون علمه علاوة على ذلك فأنها تفهرس وتنشر وتستثمر دون تمكين صاحب البيانات من ممارسة حقوقه عليها .ويذهب البعض الى انه " اذا لم تؤد خدمة على شبكة الانترنت فانك لن تكون مستهلكا وانما المنتج المباع "[1]، والملاحظ ان البيانات الشخصية اضحت محلا للاتجار بها من قبل المواقع والشركات ، بل يمكن القول انها تمثل محلا لاقتصاد جديد ، وذلك لسهولة جمعها وانخفاض تكاليفها ، وهو ما ادى الى قيام الكثير من الشركات التجارية الى العمل في مجال جمع وبيع البيانات الشخصية وهو ما اصبح يسمى ب " التسويق الالكتروني "[2] . فالمواقع والشركات الالكترونية تقدم خدمات مبتكرة ومجانية في الغالب ، لكن مقابل الاستغلال التجاري للبيانات الشخصية

ويتم ايضا استخدام البيانات الشخصية للاغراض التجارية بعد تجميعها من خلال شبكة الانترنت عن طريق ملفات كوكيز التي سبق الاشارة اليها [3]، حيث يقوم الموقع الخاص بالمنشأة التجارية بزرع هذه الملفات الى القرص الصلب للكمبيوتر الخاص بمستخدم الانترنت عند زيارته للموقع . وهذه الملفات تقوم بتخزين العديد من المعلومات والبيانات عن الزبون مثل المواقع التي يقوم بزيارتها ، والمنتجات التي يفضلها ، اضافة الى اسمه وعنوانه الالكتروني وغيرها من البيانات التي يقوم المستخدم بكتابتها اثناء

---

[1] د. جبالي ابو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية ، بحث مقدم الى مؤتمر العصر الرقمي واشكالياته القانونية ، المنعقد في كلية الحقوق جامعة اسيوط ، الفترة من 12-13 نيسان ، 2016 ، ص30 .

[2] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، القسم الاول ، مصدر سابق ، ص400.

[3] د. جبالي ابو هشيمة كامل ، مصدر سابق ، ص 31 .

دخولـه الى شـــبكـة الانترنـت . وبعد ان تقوم هذه الملفات بتخزين البيانات ، ترســـلها الى الموقع الخاص بالشركة التجارية ، التي تستطيع من خلالها ارسال عروض تجارية ودعائية خاصـة للزبون تتناسب مع ميوله واذواقه وافضلياته .

الفصل الثاني

الاحكام المنظمة لعلاقة الشركات المالية مع الزبون

ندرك بأن البيانات اصبحت في الوقت الحاضر ركيزة من ركائز التنمية وحجر اساس في المنظومة التشريعية للبلدان ويعود ذلك لاهميتها الاجتماعية والسياسية والاقتصادية والامنية ، ومن جهة اخرى ادى تطور وسائل الاتصال الحديثة الى ازدياد اهمية المعلومات لسهولة الحصول عليها ، الا ان تداولها والاتجار بها يحتاج لوجود تنظيم قانوني ينظم نشاط تداولها كخدمة الكترونية وحمايتها من الاستغلال والاعتداء عليها .

وقد تبدو حماية البيانات الشخصية من اكثر من جانب سواء في حالة التصرف فيها وتنظيم العقد لهذه الحماية او من جانب القانون حينما لا يكون هناك اتفاق او اجازة من قبل الشخص الذي تعود له هذه البيانات (الزبون) للشركة المعنية ، وأيضا انه من اللازم معرفة الضمانات الضرورية للمحافظة على بيانات الزبائن خصوصا كون التعامل بها كما مرة سابقا انتشر بشكل كبير في البيئة التجارية الالكترونية في السنوات السابقة وهو ما سنتناوله في هذا الفصل وكالاتي : المبحث الاول : علاقة الشركات المالية باصحاب البيانات الشخصية ، اما في المبحث الثاني : الضمانات القانونية لحماية البيانات الشخصية ، وكالاتي .

المبحث الاول

علاقة الشركات المالية باصحاب البيانات الشخصية

تقوم الشركات المالية بالعديد من الخدمات لزبائنها ، وعادة ما تتولد عن ذلك علاقة مباشرة تسمح لهذه الشركات بالحصول على بيانات الزبائن الشخصية ، وكما مر علينا سابقا ان هذه البيانات اصبحت لها قيمة مالية كبيرة تكون بذاتها مطمع للشركات في التصرف بها والحصول على مردود مالي معتبر جراء هذه التصرف ، ولكن بالوقت نفسه عليها الحفاظ على خصوصية هذه البيانات حال التعامل معها ، وبناء عليه سنتناول هذا المبحث في مطلبين نتناول في الاول حق الشركة في التصرف ببيانات زبائنها ، وفي الثاني سنتناول التزام الشركات المالية بالخصوصية في التعامل مع البيانات الشخصية للزبائن وكالاتي .

المطلب الاول

حق الشركة في التصرف ببيانات زبائنها الشخصية

كان للتقدم الرقمي الذي حدث في عالم اليوم تأثيرا كبيرا على البيانات الشخصية وعلى اساليب استغلالها وخاصة في مجال حق الشركة بالتصرف في بيانات زبائنها بشكل مباشر ، فجمع وتخزين وعرض ونقل البيانات غاية في السهولة والسرعة والاتقان وبأقل التكاليف ، وما ساعد في تغير اسلوب استغلال البيانات هو عملية النسخ والنقل التي تتم الان باستخدام احدث التكنولوجيات من خلال شبكة الانترنت والتي كانت في السابق تتم باسلوب تقليدي غير متقن وبكلفة عالية .

فاصبح لزاما الاستجابة للتطورات التقنية الحديثة من حيث التشريعات التي يجب ان تتوائم معها ، وعلى هذا قننت بعض الدول التشريعات الخاصة بهذا النوع من التعامل ، فسمحت للشركات المعنية بالتصرف في هذه البيانات في حالات معينة وبموجب القانون ،في حين اشترطت وجود عقد بين الشركة وصاحب البيانات في حالات اخرى وهو ما سنتناوله في الفرعين الاتيين وكالاتي .

الفرع الاول

حق الشركة بالتصرف ببيانات زبائنها قانونا

اذا كان الاصل انه لا يجوز للشركات نقل بيانات الزبائن والتصرف بها الى الغير[1]، الا ان هذا الاصل يرد عليه عدة استثناءات وان كان يؤكد المشرع المصري وفقاً لنص المادة الثانية من قانون حماية البيانات الشخصية المصري التزام المتحكم بالحفاظ على البيانات الشخصية وعدم إتاحتها إلا في الأحوال التي يصرح بها القانون، ويتفق في ذلك مع اللائحة العامة التي تؤكد ذلك سواء في المادة الرابعة أو المادة الخامسة. بيد أن صياغة النص جاءت غير منضبطة، فهي توحي في البداية بالتزامه بالعمل أو الامتناع عن عمل من شأنه إتاحة البيانات ثم عاد وقصرها على الأحوال المصرح بها قانوناً، فكان من الأولى أن يستهل الفقرة بكلمة "عدم" القيام بعمل ... إلا في الأحوال المصرح بها قانوناً، كما كان يمكن إضافة " أو موافقة صريحة من الشخص المعنى بالبيانات"، اتساقاً مع المادة 2 من قانون حماية البيانات الشخصية المصري بشروط جمع ومعالجة البيانات. وهذه الاستثناءات هي

اولا : التشخيص الرقمي لبيانات الزبون ، ويعرفه جانب من الفقه بانه " تحديد ملامح الحالة الشخصية للفرد من خلال معالجة الآلة او النظام للبيانات المتاحه عنه رقميا ، سواء كان الهدف من وراء ذلك تحقيق مصلحة خاصة او عامة " [2] ، في حين عرفته اللائحة الاوربية العامة لحماية البيانات بانه (اي شكل من اشكال المعالجة الالية للبيانات الشخصية المشتملة على استخدام البيانات الشخصية لتقييم بعض الجوانب الشخصية المتعلقة بشخص طبيعي ، وعلى وجه الخصوص التحليل او التنبؤ بالجوانب المتعلقة باداء ذلك الشخص في العمل ، الوضع الاقتصادي ، الصحة ، الميول الشخصية ، المصالح ، الموثوقية ، السلوك ، الموقع او التحركات)[3] وممكن ان تضاف لها البيانات التي تستحصلها الشركة نتيجة انتفاع الزبون بالخدمات الرقمية واستخدام الاجهزة التكنولوجية ، مثال ذلك تاريخ تصفح الزبون للمواقع الالكترونية ، وكلمات السر الخاصة بحساباته الشخصية وغير ذلك ، ويذهب البعض الى ان البيانات التي تستخلصها او تستنتجها الشركة لا تدخل في نطاق حق الفرد في منع نقل البيانات الشخصية الا بموافقته التحريرية ، مثال ذلك تقييم الحالة الصحية للشخص من خلال بياناته الشخصية المتوفرة او تقييم حالته المالية ، ويترتب على ذلك ان الملفات الشخصية للفرد ، الناتجة عن عملية التشخيص الرقمي ، والتي توضح الجوانب الشخصية له لا تدخل في اطار الحق في قابلية الفرد في نقل بيانته الشخصية بارادته[4] .

وعلى الرغم من ان الملفات الشخصية التي اعدتها الشركة موضوع البيانات الشخصية والناتجة عن عملية التشخيص الرقمي لا تدخل في حق صاحبها في منع نقل البيانات الا بموافقته التحريرية وفقا للائحة

---

[1] رضوان اسخيطة ، اضاءة على اللائحة العامة الاوربية لحماية البيانات الشخصية ، 2018 ، ص15 .

[2] د. هيثم السيد احمد عيسى ، التشخيص الرقمي لحالة الانسان في عصر التنقيب في البيانات عبر تقنية الذكاء الاصطناعي ، وفقا للائحة الاوربية العامة لحماية البيانات لعام 2016 ، دار النهضة العربية، القاهرة ، 2019، ص17 .

[3] الفقرة 4 من المادة 4 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .

[4] رضوان اسخيطة ، مصدر سابق ، ص18.

الاوربية (GDPR) الا ان هذا الحق مع ذلك يرتبط بعملية التشـــخيص الرقمي من زاوية ان هذه العملية تمر بأكثر من مرحلة قبل الوصول الى النتيجة النهائية لها ، اي قبل الوصول الى تقييم الجوانب الشخصية للفرد موضوع البيانات ، فكما بينا سابقا يتم تجميع البيانات وتخزينها واعدادها قبل تحليلها وتطبيق الملفات الشخصية الاولية الناتجة عن ذلك ، وتدخل هذه البيانات المستخدمة في المراحل السابقة على عملية التقييم النهائية في اطار حق الفرد في منع نقل بياناته الشخصية الا بموافقته وفقا للائحة الاوربية .

ويرى الباحث عدم صحة توجه المشرع الاوربي (GDPR) اذ انه لم يشمل نطاق حق الشخص في منع نقل بياناته الشخصية ، البيانات المستخلصة او المستنتجة من قبل الشركات ، لكي يتمكن الزبون موضوع البيانات الشخصية من التحكم في بياناته الشخصية ليس فقط في صورتها الاولية ولكن ايضا بعد تحليلها ، بحيث يكون له الحق فيما يتعلق بعملية التشخيص الرقمي ، في استلام ملفاته الشخصية التي تحتوي على تقييم للجوانب الشخصية له ، خصوصا ان التشخيص الرقمي هو صورة من صور المعالجة الالية للبيانات الشخصية ، والتي اقرها المشرع الاوروبي ، ولذا كان يجب عدم استبعادها من نطاق اي من الحقوق التي تمكن الفرد موضوع البيانات من التحكم في بياناته الشخصية.

ثانيا : البيانات التي لا يشـكل افشـائها او نقلها تهديد لكرامة او اعتبار من تخصـه هذه البيانات او لحياته الخاصـة : من المعلوم ان المشـرع الاوربي فرض التزاما على عاتق الشـركة بعدم افشـاء بيانات الزبون الشخصية للغير ، اذا كان في افشاء هذه البيانات ما من شأنه ان يهدد اعتبار صاحب الشأن فيها او حياته الخاصـة ، كالبيانات المتعلقة بالوضـع المالي او المعتقد وغيرها ، وهذا الالتزام لم يرد في قانون حماية البيانات الشخصية المصري ، وانما ورد في قانون العقوبات ، اذ وضع المشرع عقوبة جنائية على معالج البيانات في حال مخالفته لهذا الالتزام ، وذلك في المادة (226) من قانون العقوبات المصري رقم 58 لسنة 1937 المعدل .

ثالثا : نقل البيانات والتنازل عنها لضـرورة قانونية : اذا كان من الثابت ان الالتزام بعدم نقل او التصـرف بالبيانات الشخصية من جملة الالتزامات والواجبات الملقاة على عاتق الشركات ، وهو ما ذهب له المشرع المصـري بموجب قانون مكافحة جرائم تقنية المعلومات ، واورده في البند (2) من الفقرة (اولا) من المادة (2) بقوله " يلتزم مقدمو الخدمات بالمحافظة على سرية البيانات التي تم حفظها وتخزينها ، وعدم افشائها او الافصـاح عنها بغير امر مسبب من احدى الجهات القضـائية المختصة ، ويشمل ذلك البيانات الشخصية لاي من مستخدمي خدمته ، او اي بيانات او معلومات متعلقة بالمواقع والحسابات الخاص التي يدخل عليها هؤلاء المستخدمون ، او الاشخاص والجهات التي يتواصلون معها " .

وقد فرض المشـرع المصـري الالتزام ذاته على عاتق كل من المتحكم والمعالج في قانون حماية البيانات الشـخصـية ، وذلك في البند (5) من المادتين (4،5) منه على التوالي بقوله " يلتزم المتحكم او المعالج القيام بعمل او الامتناع عن عمل يكون من شأنه اتاحة البيانات الشخصية او نتائج المعالجة الا في الاحوال المصرح بها قانونا ". ونلاحظ ان المشرع المصري فيما عدا حالة موافقة الشخص المعني على الكشف عن بياناته الشخصية ، عالج حالات السماح بأفشاء البيانات الشخصية او اتاحتها او الافصاح عنها في قانون حماية البيانات الشـخصـية بطريقة مختلفة عن قانون مكافحة جرائم تقنية المعلومات المصـري ، فجعلها في هذا الاخير بناء على امر مسبب من احدى الجهات القضائية المختصة ، في حين تركها لتقديره في قانون حماية البيانات الشخصية. وهناك استثناءات اشارت اشارت لها قوانين بعض الدول [1].

[1] ومن الاستثناءات في الولايات المتحدة الامريكية ترجيح المصلحة العامة على المصلحة الخاصة في بعض حالات نشر المعلومات المتعلقة بالحالة الجنائية للشخص ، وهذا ما اكده القضاء الامريكي ، فذهبت محكمة الاستئناف الدائرة الاولى في

يُشار إلى سابقة رفض لجنة الاتصالات وتكنولوجيا المعلومات بمجلس النواب ووزارة الاتصالات طلب البنك المركزي باستثنائه والجهات التابعة له من مشروع قانون "حماية البيانات الشخصية المصري"، تأسيساً على أن القطاع المصرفي في العالم يخضع لحماية مضافة للبيانات لأنها بطبيعتها بيانات حساسة، وأن فلسفة مشروع القانون تكمن فى تنظيم حماية البيانات وليس وضع سرية على البيانات. ونعتقد بأن هذا الاستثناء يُفرغ القانون من مضمونه ويجعله بلا قيمة ويمثل عدم استيعاب لفلسفة حماية البيانات الشخصية التي تعد حقًا أصلياً للمواطن. ولكن ظهر القانون فى النهاية بعد مناقشته فى المجلس متضمنا هذا الاستثناء [1]. وذهب مشروع قانون حماية تكنولوجيا المعلومات وحماية البيانات ذات الطابع الشخصي اللبناني الى جواز الترخيص الاجباري لنقل البيانات الشخصية والتصرف بها في حالات ثلاث وهي :

1- امن الدولة او الدفاع الوطني او الامن العام .
2- الجرائم الجزائية او الدعاوى القضائية
3- الحالات الصحية او الهوية الوراثية او الحياة الجنسية

بحيث حصر هذا المشروع الترخيص بالنسبة للحالة الأولى بقرار يصدر من وزيري الدفاع الوطني والداخلية ، اما الحالة الثانية فقد حصرها بقرار يصدر عن وزير العدل ، اما الحالة الثالثة فبقرار يصدر عن وزير الصحة [2] .

ويثير هذا الامر تحديات عديدة لا سيما بالنسبة للشخص صاحب البيانات التي يرد الترخيص عليها ، وان توقيف الاذن او الترخيص على قرار يصدر عن وزير العدل من شأنه ان يعيق عملية البحث العلمي والاحصائي التي يجب ان تراعي خصوصية الافراد وبياناتهم الشخصية المتعلقة بالنزاعات القضائية ، والتي تتطلب حذف أسماء المعنيين في الدعاوى القضائية على سبيل المثال[3] .

كما ان غياب المعايير الواضحة التي تساعد وزير العدل في اتخاذ قرارات رشيدة قد يعيق عملية المعالجة القانونية وغير التعسفية للبيانات ذات الطابع الشخصي . وبدلا من انشاء هيأة وطنية مستقلة تمارس الاشراف والرقابة على عملية نقل البيانات والتصرف بها ، حصر هذا المشروع الترخيص بموافقة السلطة العامة دون الاعتداد برأي الشخص المعني بالمعلومات دون تحديد دوره وحقوقه .

حكمها الصادر في (18) ابريل 2014 في القضية الخاصة برفض جهات انفاذ القانون الكشف عن اسماء وعناوين ستة اجانب كانت قد صدرت ضدهم احكام جنائية سابقة ، فطالبت صحيفة (Union Leader) بالزام هذه الجهات بالكشف عن هذه المعلومات طبقا لما هو مقرر في قانون حرية المعلومات (FOIA) وذهبت المحكمة الى ان قانون حرية المعلومات قد استثنى الكشف عن مثل هذه المعلومات ، وبالتالي لا يعتبر انتهاكا للخصوصية في حال الكشف عن اسماء المعتقلين وعناوينهم ، ورأت المحكمة ان المصلحة العامة في الافصاح عن هذه المعلومات تفوق المصلحة الخاصة للأشخاص.

Union Leader Corp0ration .v. U.S. DEPT. Of Homeland, Security , U.S . Immigration and Customs Enforcement. United States of Appeals , First Circuit , No . 13 – 1752 , Decided : April 18 m 2014 , Available at : http // canlaw : findlanv : com/ us – lst – circuit / 1663921.html (Visited on January 15 ,2017 .

[1] د. خليف مصطفى ، الحماية القانونية للحق في الحياة الخاصة ، ط1 ، مكتبة الوفاء القانونية ، مصر ، الاسكندرية ، 2021 ، ص66 .

[2] د. محمد محمد القطب مسعد ، مصدر سابق ، ص831.

[3] د. خالد حسن ، مصدر سابق ، ص 82 .

الفرع الثاني

حق الشركة بالتصرف بمعلومات زبائنها وفق العقد

تقرر فيما سبق اعتبار حق صاحب البيانات على بياناته الشخصية حق ملكية بالمعنى القانوني ، كما تقرر اعتبار هذه البيانات داخلة في مفهوم المال عند اغلب الفقه .

وأيضا يعد محتوى البيانات الشخصية من الحقوق المالية ، وهي الحقوق التي تقَوم بالمال فيكون محلها مالا ، او مقوم بالمال ، وتنظم العلاقات المالية بين الشخص وغيره وسميت بالحقوق المالية لانها تنتج غالبا عن المعاملات المالية بين الأشخاص وتتميز عن سائر الحقوق الأخرى بانها تقبل التنازل ، وتقبل الانتقال من شخص الى اخر ، وبصلاحياتها لان تكون محلا للتعامل ، مالم يمنع ذلك قانون[1].

واذا كان من الثابت ان للتكنولوجيا المعلوماتية دور في اتمتة اعمال المصارف وتحويل الاموال الكترونيا ، ونظم معلومات اسواق الاوراق المالية وتجهيز المصانع والتصاميم بواسطة الكمبيوتر ، وفي قطاع المواصلات والشبكات الرقمية والبرمجيات المساندة للتعليم والتعلم والتدريب من خلال المحاكاة ونظم المعلومات التربوية وغيرها الكثير ، فأنه من باب اولى امكانية التصرف في البيانات الشخصية للافراد من الحائز الى الغير بناء على موافقة الشخص المعني بالبيانات ، اذ اعطت اللائحة الاوربية الحق لصاحب البيانات في السماح بنقلها الى الغير، في حين أغفل المشرع المصري النص على حق الشخص المعني بالبيانات في نقل البيانات الشخصية الخاصة به، رغم أنها من الحقوق المهمة[2] ، ولم يفوت المشرع الأوروبي النص على هذا الحق في إمكانية نقل البيانات Right to data portability في اللائحة الأوروبية حيث تضمنها نص المادة 20 منها، الذى يجري على أن يكون للشخص المعني بالبيانات الحق في استرداد بياناته الشخصية التي قدمها إلى الشخص المسؤول بتنسيق منظم ومعروف ويمكن قراءتها آليًا. وبالإضافة إلى ذلك، لديه الحق في نقل هذه البيانات إلى شخص آخر مسؤول عنها دون عائق من قبل الشخص المسؤول الاول عن تجميع البيانات الشخصية وعالجتها، شريطة أن: تعتمد المعالجة على الموافقة على النحو الوارد فى المادة 6 الفقرة 1 البند (أ) من اللائحة أو المادة 9 الفقرة 2 البند(أ)من اللائحة أو بعقد وفقًا للمادة 6 الفقرة 1 البند (ب) من اللائحة.

و تتم المعالجة بوسائل آلية. وبممارسة هذا الحق، يكون لصاحب البيانات أيضًا الحق في التحقق من إرسال بياناته الشخصية مباشرةً من شخص إلى آخر، طالما أن ذلك ممكن من الناحية التقنية. ولا يجوز أن تتأثر الحريات وحقوق الأشخاص الآخرين الذين تربطهم علاقة قانونية بصاحب البيانات مثل الشركة او الطرف الثاني بالمعاملة المالية . ولا ينطبق الحق في نقل البيانات على معالجة البيانات الشخصية اللازمة لأداء مهمة لأغراض المصلحة العامة أو في ممارسة السلطة الرسمية المفوضة للشخص المسؤول .[3]

---

[1] د. هيثم السيد احمد عيسى ، مصدر سابق ، ص50 .

[2] د. حسن محمد احمد حسن ، محتوى الحسابات الرقمية ومدى انتقاله للغير،ط1 ، دار الوفاء ، الإسكندرية ، 2022 ،455.

[3] د. شريف يوسف خاطر ، حق الاطلاع على البيانات الشخصية في فرنسا ، مجلية كلية الحقوق الكويتية العالمية ، العدد 9 ، السنة الثالثة ، 2015، ص233 .

واذا كان نقل البيانات داخل الدولة الواحدة لا يثير اشكاليات الا انه على العكس من ذلك اذا كان النقل لدولة خارج النطاق المكاني لتطبيق القانون تشترط المادة 15 من القانون عند نقل أو مشاركة أو تداول أو معالجة البيانات الشخصية إلى دولة لا يتوافر فيها مستوى الحماية المنصوص عليه فى القانون، ضرورة الحصول على الموافقة الصريحة للشخص المعنى أو من ينوب عنه، وهو ما بيناه سابقا .

و باعتبار أن القانون هو الذي ينشأ الحق وطريقة استغلاله، وهذا يعني بانه لا يجوز للائحة تُوضع من قبل السلطة التنفيذية (وزير الاتصالات) ان تقييد من هذا الحق مالم تستند الى قانون ، وهو ما معمول به في التوجه الأوربي ، اذ عالج الاتحاد الاوربي عملية نقل البيانات خارج اطار الاتحاد الاوربي في المادة (44 و45 و46) موضوع نقل البيانات الشخصية لاشخاص من دول الاتحاد الاوربي الى دولة او منظمة او شركة خارج الاتحاد سواء تمت معالجة البيانات ومن ثم نقلها او تم جمعها ونقلها ، ويندرج ضمن هذه المواد الشروط الاولية لصحة عملية النقل حيث تشير اللائحة الى ان النقل يجب ان يتم لدولة تصل فيها القوانين ومستوى الحماية الى المستوى المعمول به في الاتحاد الاوربي بما يضمن سلامة بيانات الاشخاص ومشروعية العمل عليها ، مما يعني ان نقل البيانات وجمعها في دولة خارج الاتحاد يجب ان يسمح به في حال اعتبرت المفوضية الاوربية الدولة هذه او الشركة التي تقع ضمن هذه الدولة لديها معايير كافية لحفظ البيانات بشكل آمن وضمن شروط اللائحة الاوربية والتي من بينها كون هذه الدولة تحترم حقوق الانسان ولديها القدر الكافي من الحريات وايضا وجود تشريعات تتعلق بحماية البيانات الشخصية ، واعطت اللائحة الحق للمفوضية الاوربية في تصنيف الحق في الدول خارج الاتحاد الاوربي وفقا للمعاير المذكورة اعلاه [1]، وان هذا التصنيف لابد وان يتم بشكل دوري نظرا للتغيرات التي قد تطرأ على الدول من حيث استيفائها للمعايير من عدمه ، وان هذه المراجعة تكون كل اربع سنوات على الاقل . واذا كانت هذه هي القاعدة العامة في عملية نقل البيانات الا انه ترد عليها بعض الاستثناءات لتوصف لنا بعض الحالات التي يمكن نقل البيانات فيها الى دول لا تتوفر فيها المعايير السابقة وهذه الاستثناءات هي :

1- يجوز نقل البيانات الى دولة خارج الاتحاد الاوروبي بالرغم من كونها ليست ضمن التصنيف الذي وضعته المفوضية الاوربية في حال كان هناك موافقة من الشخص الذي تتعلق به البيانات على الرغم من علمه كون هذه الدولة هي خارج التصنيف . وهنا يجب ان نشير الى كون اللائحة اشارت الى الموافقة مع كلمة صريحة وهذا يعني ان الموافقة لابد ان تكون بشكل واضح وصريح لا لبس فيه .
2- في حال كان هذا النقل لحماية مصالح حيوية تتعلق بالشخص صاحب البيانات او اشخاص اخرين ، او لاسباب تتعلق بالمصلحة العامة ، او في حالة كان النقل لتحقيق متطلبات ادعاء قانوني او حماية قانونية .

وان هذا الترخيص من قبل صاحب البيانات الى الشركة المعنية يستلزم توافر شروط معينة كأن يكون عن طريق التوقيع الالكتروني [2]، وان صاحب البيانات هو من يصدر الترخيص بنقل البيانات محل الاتفاق والتعاقد ، ويسمح بتسويقها حسب أسلوب استيعاب السوق ويتم الاتفاق في الغالب مباشرة بين الأطراف ، ويخضع تقدير القيم المالية للبيانات لقانون العرض والطلب ويتم ادراج ذلك في بنود التعاقد او في

[1] د. سارة علي رمال ، الحق في الخصوصية في العصر الرقمي ، منشورات الحلبي الحقوقية ، بيروت ، 2018، ص187.

[2] عرف المشرع العراقي في المادة (1/رابعا) من قانون التوقيع الالكتروني والمعاملات الالكترونية رقم 78 لسنة 2012 التوقيع الالكتروني بانه (علامة شخصية تتخذ شكل حروف او ارقام او رموز او إشارات او أصوات او غيرها وله طابع متفرد يدل على نسبته الى الموقع ويكون معتمدا من جهة التصديق)..

الاستمارة الخاصة بالموافقة على التصرف بها [1]. والاتفاق أيضا يكون شاملا عملية التخزين والحماية والاسترجاع مجتمعة نظير مبلغ يتم التراضي عليه ، ويمكن ان تكون المفاضلة بين المقابل النسبي والجزافي وذلك على أساس انه اذا سمح الزبون بنقل بيانات جميعها او جزء منها ويجوز ان يكون على أساس مشاركة نسبية في الإيراد الناتج من الاستغلال ، او قد يكون بطريقة جزافية . وممكن ان يقبل صاحب البيانات بنقلها دون مقابل مالي اذ من الممكن ان تكون هناك مردودات إيجابية أخرى غير مالية ، كالدخول الى مواقع معينة او الحصول على عروض وسلع وبرامج الكترونية مميزة وغيرها [2].

وان طبيعة التصرفات القانونية التي تتم بخصوص البيانات الشخصية ، وأسلوب التعامل معها واطراف تلك التصرفات لها خصوصية ترد عليها ويتجلى ذلك في استخدام قالب عقدي يتوائم مع تلك البيئة يظهر في شكل الكتروني ، ولصاحب البيانات وخلفه من بعده حق التصرف فيها من خلال شبكة الانترنت وبموجب عقود الكترونية .

واذا كان هذا منظم في اللائحة الاوربية لحماية البيانات الشخصية (GDBR) وقانون حماية البيانات الشخصية المصري ، الا ان البيئة التشريعية العراقية تفتقر الى هذا النوع من التشريع رغم أهميته ، اذ ان الواقع الحديث يفرض علينا تشريعا خاصا بحماية هذه البيانات وأساليب استغلالها عبر مواقع او مواطن الانترنت ، وتكون مستقلة عن الطرق التي نظمها المشرع تقليديا وذلك لاختلاف الامر من عدة وجوه واساس ذلك شبكة الانترنت والتي أصبحت سوقا ليس بحجم السلع والخدمات فحسب ولكنه غير محدود بحدود جغرافية او محدود بزمن او وقت واحد سلع تلك السوق هي البيانات الشخصية لزبائن الشركات المالية ، وذلك بعد تثبيتها المادي على دعامات اليكترونية وعرضها على شبكة الويب بعد ان أصبحت ضمن برمجيات الحواسيب، فموضوع البيانات الشخصية بشكل يبين استقلالها في التعاملات عليها مقارنة بالسلع العادية مما يؤكد ضرورة إيجاد قانون خاص بها نظرا للحاجة الماسة [3]. وهذا التصور لم يأتي من فراغ فهناك اختلاف كبير بين الطريقة التقليدية العادية والطرق الرقمية الحديثة في تداول البيانات الشخصية ومختلف السلع الالكترونية من حيث مفردات كثيرة مثل النشر والتسويق والعرض وشكل السوق وحجمه وطريق البيع والشراء والتعاقدات وأسلوب الدفع ومن حيث السرعة والانتشار ، وفي مدى الالتزام بالثوابت والأخلاق ومدى الحفاظ وصيانة الخصوصية والمعلومات ومن حيث شكل الاعتداء والسرقة واختلاف طرق التأمين وتأثير المعلوماتية عليها بصفة خاصة .

المطلب الثاني

التزام الشركات المالية بحق الخصوصية في التعامل مع البيانات الشخصية للزبائن

أصبحت البيانات الشخصية محلا للتعامل بين الشركات التي تقوم بجمعها ، فكل شركة تقوم بتبادل البيانات التي جمعتها عن زبائنها مع شركات أخرى ، وذلك بهدف الوصول الى بيانات متكاملة عن كل زبون ، ويمكن ان يشكل ذلك خطرا على خصوصية الافراد ، اذ ان الفرد قد يقوم بمنح بعض البيانات لشركة او جهة معينة في حدود ما هو ضروري لتقديم خدمة له ، ويعتقد ان هذه البيانات لا تسمح برسم صورة كاملة

[1] د. فؤاد الشعيبي ، التنظيم القانوني لعقود خدمات الاتصالات ، ط1، منشورات الحلبي الحقوقية ، بيروت ، 2014 ، ص 426 .

[2] د. محمد مختار مختار فودة ، قانون التجار الدولي في المعاملات الالكتروني ، دار النهضة العربية ، القاهرة ، 2022 ، ص 106.

[3] د. محمد مختار مختار فودة ، المصدر نفسه ، ص179 .

عنه ، ولكنه لا يعلم ان هذه البيانات قد يتم تكملتها ببيانات أخرى قام بتقديمها هو قبل ذلك او لشركة أخرى ، مما يؤدي الى رسم صورة متكاملة له [1]، ويزداد هذا الخطر مع سهولة نقل البيانات عبر الشبكات المختلفة نتيجة لعدم قدرة بعض الشركات على توفير الأمان الكامل لسرية ما ينقل عبرها من معلومات ، وإمكانية استخدام هذه الشبكات في الحصول عليها بصورة غير مشروعة كالتجسس الالكتروني [2]،فقد أتاح تكامل عناصر الحوسبة مع الاتصالات والوسائط المتعددة وسائل رقابة متطورة سمعية ومرئية ومقروءة ، إضافة الى برمجيات التتبع وجمع المعلومات اليا ، كما اتاحت شبكة الانترنت القدرة العالية لا على جمع المعلومات فقط بل معالجتها عبر تقنيات الذكاء الاصطناعي التي تتمتع بها الخوادم ، والتي تتوفر أيضا لدى محركات البحث وبرمجيات التحليل والتصرفات على الشبكة ، بحيث لا يستغرب معها ان الشخص عندما يتصل بأحد مواقع المعلومات البحثية في هذه الأيام يجد امامه المواقع التي كان يفكر في دخولها والتوصل بها ، كما لا يستغرب مستخدم الانترنت ان ترده رسائل بريد الكتروني تسويقية تغطي ميوله ورغباته من جهات لم يتصل بها . والأكثر خطرا من ذلك كله ان البيانات الشخصية أصبحت اليوم محلا لاقتصاد جديد ، ومحلا للاتجار بها من قبل الشركات التي تقوم بجمعها من اجل جلب المال لهذه الشركات [3]. وعليه فمن الضروري التزام الشركات بالحفاظ على البيانات الشخصية للزبائن وعدم اتاحتها لشركات اخرى الا في الأحوال التي يجيزها العقد او القانون كما بينا ذلك مسبقا ، والأخيرة ينبغي التقيد بحدودها سواء كانت إجازة قانونية او اتفاقية، اما اذا لم تكن هناك اجازة فانه يمنع على الشركات المعنية التصرف في تلك البيانات ، ويجب عليه الالتزام بالخصوصية وهو ما سنتناوله تباعا .

الفرع الأول

الالتزام بالخصوصية في حالة الاجازة

رأينا انه بإمكان صاحب البيانات السماح للشركة المعالجة بنقل بياناته الى شركات أخرى ، وعادة ما تأخذ هذه الاجازة صيغة عقد ، ويجب ان يتضمن العقد بعض المعلومات والالتزامات الخاصة ، ولكن مع ذلك تبقى بعض الالتزامات القانونية التي تقع على شركة لغرض المحافظة على الخصوصية وهذه الالتزامات هي :

أولا : التزام الشركة بالسماح للزبون في الاطلاع على بياناته وتصحيحها ، بداية يجب القول بأن حق صاحب البيانات في الاطلاع عليها اطلقت عليه بعض التشريعات تسمية حق النفاذ او حق الوصول او الدخول اليها [4] ، كما اطلقت عليه تشريعات أخرى حق الولوج [5] . ويعرف هذا الحق بانه حق صاحب البيانات التي جمعت النفاذ والوصول اليها وتحديثها ، دون قيود وعلى فترات ودون تأخير مفرط وبلا أعباء مالية ، ويشمل هذا الحق الدخول الى جميع مواقع البيانات الشخصية المتعلقة به [6]. كما يشمل حق

---

[1] د. فؤاد الشعيبي ، مصدر سابق ، ص 195.

[2] د. سليم عبد الله الجبوري ، الحماية القانونية لمعلومات شبكة الانترنت ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2011 ، ص 332.

[3] د. محمد مختار مختار فوده ، مصدر سابق ، ص 203.

[4] See article 15 of Regulation (EU) 2016 / 697 of the European .

[5] كما هو الحال في قانون حماية الأشخاص الذاتيين نجاه معالجة المعطيات ذات الطابع الشخصي رقم 8 لسنة 2009 حيث اشارت الى تفصيلات الحق في الولوج المادة 7 منه .

[6] د . عمرو طه بدوي ، التنظيم القانوني لمعالجة البيانات الشخصية ، مصدر سابق 128 .

النفاذ الحق في الحصول على نسخة من البيانات بلغة واضحة ومطابقة لمضمون التسجيلات وبطريقة مبسطة اذا تمت معالجتها اليا [1].

وقد اعطى القانون الفرنسي الشخص الطبيعي محدد الهوية الحق في الاتصال بالشركة المعنية للاستعلام عن بياناته الشخصية وان يطلب منها مايلي[2] :

1- التأكد مما اذا كانت بياناته الشخصية تخضع للمعالجة الالية او اليدوية من عدمه .
2- المعلومات المتعلقة باهداف المعالجة والبيانات الشخصية محل المعالجة ومجموعة المستفيدين الذين تم الإفصاح عن بياناتهم .
3- المعلومات الخاصة بنقل البيانات الشخصية .
4- الاطلاع على البيانات الشخصية لصاحب الشأن او اية معلومات متاحة من قبله .

وان نطاق هذا الحق يشمل كافة البيانات والمعلومات الشخصية المخزونة والمعالجة والتي تخص الشخص الطبيعي ، ويجب على الشركة وبناء على طلب من الشخص الذي جمعت بيانته تمكينه فور طلبه من النفاذ الى بيانته الشخصية وتحديثها ، ويشمل هذا الحق الدخول الى كافة المواقع الالكترونية المتعلقة بالبيانات الشخصية للشخص المعني ، وعليها وضع الوسائل التقنية المناسبة لتمكينه من ذلك بطريقة الكترونية [3].

والالتزام بالسماح على الاطلاع على البيانات الشخصية أكدته اللائحة الاوربية وجاء تحت عنوان حق صاحب البيانات في الاطلاع عليها [4]، حيث نصت على ان يكون لصاحب البيانات حق الوصول الى بيانته والتعرف على المعلومات الاتية : (..... فئات واصناف البيانات الشخصية ، والمستفيدين منها ، الفترة المتوخاة لتخزين البيانات ....).

وهذا الالتزام يتحلل الى امرين أولهما يتعلق بحق صاحب البيانات في الاطلاع والتعرف على عدة أشياء منها على سبيل المثال : طبيعة البيانات ، وغايتها ومصدرها ، وثانيهما يتعلق بحقه في طلب تصحيح ما شاب البيانات من أخطاء اثناء عملية المعالجة ، باعتبار ان ما يعتبر حق للزبون هو واجب على الشركة .

1- : بالنسبة لحق صاحب البيانات في الاطلاع على بياناته ، بموجب هذا الحق يستطيع صاحب البيانات او ورثته او وليه الاطلاع على جميع بياناته الخاصة ، ويتعين على هؤلاء الأشخاص ممارسة هذا الحق في اجال معقولة وبطريقة غير مرهقة [5] ، ولا يجوز لهم التنازل مسبقا عن هذا الحق او الحد منه الا في حالات محددة [6] ، وكما بينا فانه يخول حق الاطلاع لصاحب

---

[1] وهذا ما نصت المادة 32 من قانون حماية المعطيات التونسي لسنة 2004 ، اذ ذكرت بانه (يقصد بحق النفاذ على معنى هذا القانون حق المعني بالامر او ورثته او وليه في الاطلاع على جميع المعطيات الشخصية الخاصة به وطلب إصلاحها او اتمامها او تعديلها او تحيينها او تغييرها او توضيحها او الشطب عليها اذا كانت غير صحيحة او غامضة او كانت معالجتها ممنوعة).

[2] انظر نص المادة 39 من قانون حماية البيانات الشخصية الفرنسي لسنة 1978 والمعدل عام 2004 .

[3] د. طارق جمعة السيد راشد ، مصدر سابق ، ص75 .

[4] انظر نص المادة 13 من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016

[5] الفصل الرابع والثلاثون من قانون حماية المعطيات الشخصية التونسي رقم 63 لسنة 2004 .

[6] وقد تعرضت بعض التشريعات الى هذه الحالات منها على سبيل المثال القانون التونسي حيث نص الفصل الخامس والثلاثون من القانون اعلاه على ان : "لا يمكن الحد من حق المعني بالامر او ورثته او الولي في النفاذ الى المعطيات الشخصية المتعلقة به الا في الحالات الاتية ، اذا كانت معالجة المعطيات الشخصية لأغراض علمية وبشرط ان يكون مساس المعطيات الشخصية بالحياة الخاصة محددا . اذا كان القصد من الحد من النفاذ حماية المعنى بالامر نفسه او الغير ".

البيانات الحق في الحصـول على نسـخة من بيانته بلغة واضـحة ومطابقة لمضـمون التسـجيلات وبطريقة مبسطة متى تمت معالجتها اليا . على انه يتم اصدار النسخة لمقدم الطلب بناء على طلبه بعد التثبت من هويته ، وللشـركة ان تمتنع عن الاسـتجابة للمطالبة التعسـفية التي تظهر بشـكل واضـح من خلال عددها وتكرارها ، ويجوز للمراقب فرض رسـوم معقولة على أسـاس التكاليف الإدارية [1] .

وفي بعض الأحيان قد يرفض المسؤول عن المعالجة او المعالج تمكين المعني بالامر او ورثته او وليه من الاطلاع على البيانات او تأجيل طلبه بالاطلاع عليها او عدم تسـليمه نسـخة من البيانات . في هذه الحالة يجوز لهؤلاء الأشخاص ان يقدموا طلبا الى الجهة الإدارية المختصة في اجل معين يبدأ من تاريخ الرفض . وعلى تلك الجهة بعد سماع الطرفين واجراء التحريات اللازمة الاذن بالاطلاع على البيانات المطلوبة او بتسـليم نسـخة منها او المصـادقة على الرفض ، وذلك خلال اجل معين ، وفي الوقت ذاته يجوز للمعني بـالامر او ورثتـه او وليـه عند الاقتضـاء تقديم طلب الى الجهة الإدارية لاتخاذ جميع التدابير الكفيلة بمنع اتلاف البيانـات او اخفائها ، وعلى الجهـة المختصـة البت في الطلب خلال فترة زمنية معينة من تاريخ تقديمه ، ويترتب على تقديم الطلب من اتلاف البيانات او اخفائها [2].

2- : بالنسـبة لحق صـاحب البيانات في طلب تصـحيحها اذا ماشـاب البيانات أخطاء ، حيث قد تقع الشركة اثناء قيامها بجمع المعلومات او معالجتها او نقلها في بعض الأخطاء ، ولبيان مواجهة هذه الفرضية ؟.

يجد الباحث انه وبعد الرجوع الى التشـريعات المعنية بحماية البيانات الشـخصـية ، ان البعض منها اقرت لصاحب البيانات او من ينوب عنه او وليه الحق في تصحيحها ، او اكمالها اذا كان يشوبها نقص او تعديلها او تغييرها او شطبها اذا كانت غير صحيحة او غامضة او كانت معالجتها ممنوعة [3].

ولتمكين الشـخص المعني بالامر او ورثته او وليه من تقديم طلب تعديل بياناته الشـخصـية او تغييرها او إصـلاحها ، اتجهت بعض التشـريعات الى الزام الشـركة وضـع كافة الإمكانيات التقنية اللازمة لتمكين الزبائن من ارسال مطالبهم بطريقة الكترونية [4].

كما يجب ملاحظة ان الاعتراف للزبون صاحب البيانات بالحق في تقديم طلب تصحيح بيانته ، يجد أساسه القانوني في الاعتراف له في أي وقت الوصول الى بياناته وطلب مراجعتها .

---

[1] الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، ص77 .

[2] وقد أجاز المشرع الفرنسي في المادة 39 من قانون المعلوماتية والحريات الفرنسي رقم 78 لسنة 1978 والمعدل باحكام القانون رقم 804 لسنة 2004 في حالة حدوث خطر إخفاء او اختفاء البيانات الشخصية يجوز للمحكمة المختصة ان تأمر بما في ذلك الدعاوى المستعجلة ، باتخاذ كافة التدابير لمنع مثل هذا الاخفاء او الاختفاء .

[3] الحق في تصحيح البيانات حق اقرته المادة 16 من اللائحة الاوربية رقم 679 لسنة 2016 ، حيث اقرت فيها لصاحب البيانات ان يحصل من المراقب دون تأخير لا مبرر له على تصحيح البيانات الشخصية المتعلقة به وغير الدقيقة ، ويكون له الحق في تكملة بياناته الشخصية عن طريق تقديم بيان تكميلي .

[4] انظر الفصل السابع والثلاثون من قانون حماية المعطيات الشخصية التونسي رقم 63 لسنة 2004 .

وتصحيح البيانات قد يتحقق من خلال القيام بتقديم صاحب البيانات او نائبه القانوني طلب تصحيح البيانات ، ويتعين على الشركة اخطار كل متلق للبيانات بما تم عليها [1]. كما يتعين ان يتم تصحيح البيانات خلال مدة وجيزة حددتها بعض التشريعات بعشرة أيام [2].

وفي بعض الأحيان قد يتم رفض طلب التصحيح او لم تتم الاستجابة له خلال الاجل المذكور في هذه الحالة يجوز للشخص المعني بالامر (صاحب البيانات) إيداع طلب التصحيح لدى الجهة الإدارية المختصة ، التي تكلف احد أعضائها للقيام بكل التحقيقات التي ترى فائدة فيها والعمل على اجراء التصحيحات المناسبة ، ويجب في نفس الوقت إبقاء الزبون على اطلاع بالمآل المخصص لطلبه .

ثانيا : حق العدول عن الموافقة على الاحتفاظ بالبيانات : يشترط القانون المصري، في مادته الثانية، ضرورة صدور موافقة صريحة من الشخص المعنى بالبيانات على عمليات جمع البيانات أو معالجتها، إلا في الأحوال المصرح بها قانوناً، ومن ثم فمن الطبيعي أن يكون للشخص العدول عن هذه الموافقة، أي سحب موافقته في أي وقت، لتعلقها بحقوقه اللصيقة بشخصيته، فقد تطرأ أمور خاصة لدى الشخص تستدعي عدم الاحتفاظ بالبيانات أو معالجتها. ويصدر طلب العدول من الشخص أو من كل ذي صفة قانونية(كالورثة أو من ينوب عنه) ويوجه للمتحكم أو المعالج أو الحائز، ويجب عليه أن يبت فيه، خال فترة معقولة، ويترتب على هذا العدول عدم جواز قيام المتحكم أو المعالج بالاحتفاظ بالبيانات أو معالجتها [3].وقد أقرت اللائحة الأوروبية الحق في سحب الموافقة في الفقرة الثالثة من المادة 7 منها، فأجازت لصاحب البيانات سحب موافقته في أي وقت. بيد أن سحب الموافقة لا يؤثر على مشروعية المعالجة التي جرت بناءً على الموافقة السابقة على سحبها، على أنه يجب إبلاغ صاحب البيانات بذلك قبل إبداء الموافقة، ويجب تيسير عملية سحب الموافقة.

ثالثا : الحق في المحو (حق النسيان) تتسم شبكة الانترنت وما يرتبط بها من خوادم ضخمة تخضع لسيطرة شركات عملاقة بشراهتها لجمع وتخزين المعلومات ، وذاكرتها المطلقة التي لا يمكن محو ما يختزن فيها بسهولة من قبل الزبائن والمستخدمين ، وهو امر جعل النسيان الطبيعي امراً صعب المنال في الوقت الحاضر[4]، فهي تُحصي على مستخدميها أنشطتهم سواء كانت في شكل تعليقات أو أخبار خاصة أو صور أو معلومات شخصية ، وتجمع وتسجل بياناتهم ومعلوماتهم وتخزنها وتحتفظ بها لمدة غير محدودة، مع إتاحة هذه البيانات والمعلومات من أي مكان في العالم ولكل من يريد وفى الوقت الذى يحلو له، مع العلم أن هذه البيانات والمعلومات قد تكون قديمة أو مغلوطة أو غير صحيحة، ومع هذا تظل متاحة للجميع وعلى الدوام إلى ما لا نهاية. ومن شأن هذه المخاطر أن تسبب للشخص المعنى بالبيانات أضراراً بالغة الخطورة وتشكل تهديداً صريحاً للخصوصية، وحقهم في محو البيانات الخاصة بهم من على الانترنت، اذ ان المخاطر التي تحيط بالبيانات الشخصية تأتي نتيجة اخلال الشركة بالتزاماتها في الاحتفاظ بها بالذاكرة الحاسوبية [5]، اذ من اللازم ان يدرك كل زبون ان بياناته الشخصية سواء علق حسابه او اغلقه او توفى فأنها ستبقى منها نسخ احتياطية لدى الشركة لمدة زمنية غير معلومة ، وتستند الشركة في احتفاظها

---

[1] انظر نص المادة 19 من اللائحة الاوربية لحماية البيانات رقم 679 لسنة 2016 .

[2] حيث نصت المادة 8 من قانون حماية المعطيات الشخصية المغربي رقم 8 لسنة 2009 على ان تلتزم الشركة بالقيام بالتصحيحات اللازمة دون عوض لفائدة الطالب داخل اجل عشرة أيام كاملة .

[3] د. منى الأشقر جبور ، د. محمد جبور ، مصدر سابق ، ص146 .

[4] د. معاذ سليمان الملا ، مصدر سابق ، ص 132 .

[5] Guillaume Desgens-Pasanau,La Protection des donnees personnelles , 2Edition – 2017 , LexisNexis, Paris , p177 .

بالبيانات الشـخصـية في مثل هذه الأحوال على امرين الأول : فيما اذا علق الحسـاب من قبل الزبون قد يتراجع هذا الأخير ويعيد تنشـيطه مرة أخرى ، وكذلك الحال اذا انتهى من الخدمة فأن بياناته الموجودة تسـهل له وللشـركة أيضـا الرجوع اليها بسـهولة ، اما في حالة اغلاق الحسـاب او حذف البيانات او وفاة الزبون ، فان الشـركة تبرر احتفاظها بالبيانات بارتباطها بتعاقدات مع جهات أخرى كشـركات الدعاية و الإعلان وارتباطها أيضـا بتعاقدات مع مطورين فنيين لتحسـين مسـتوى الخدمة وهذا مالا يتناسـب مع الحذف الفوري لبيانات الزبون ، فضـلا عن تبريرها بالاحتفاظ لاعتبارات تتعلق بسـلامة الزبائن وامنهم للحد من الجرائم الالكترونية [1]، وابرز الاخطار التي ستؤول من جراء احتفاظ الشركة بالبيانات الشخصية هي :

1- تتبع الزبائن : يؤدي الاحتفاظ بالبيانات الشـخصـية الى تسـهيل عملية تقفي اثر الزبائن في المجال الالكتروني في أي وقت بسـبب ما يتركونه من اثر يتم جمعه بعد ادخال البيانات عند اسـتخدام البريد الالكتروني او في محركات البحث ، وذلك ما يسـهل تحليل أنماط الزبائن والتعرف على رغباتهم واهتماماتهم ، ليتم فيما بعد ارسال الدعايات التي تتناسب مع أفكارهم وميولهم .
2- ضـعف برامج التأمين على البيانات الشـخصـية : تعطي بعض الشـركات والمواقع الالكترونية انطباعا بقدرتها وكفاءتها التقنية على مواجهة قرصـنة البيانات وسـرقتها ، مما يعني ان تقاعسـهم في تطوير برامج الحماية سيسـهل اختراقها من قبل الهاكرز ، وهو ماحدث في إيطاليا بين عامين 2016 – 2017 حين تمت سرقة بيانات شخصية لزبائن احد اكبر البنوك [2].
3- المتاجرة بقواعد البيانات : أصـبحت عملية بيع وشـراء البيانات الشخصية كما اسلفنا سابقا من بين الأنشطة التي تجريها الشركات بشكل مستمر ، ك شركات الاتصالات والسياحة والتأمين وغيرها كنشـاط يحقق عوائد مالية ، واذا كان موضـوع الاتجار بهذه البيانات يعد من ضـمن سـياسـات الشركات سواء تم الإعلان عنها بشكل مباشر او بشكل غير مباشر ، تحت غطاء تحسين مستوى الخدمات ، فان ذلك لا يخلو من مضـار اسـتخدامها بين الأشـخاص على نحو غير مشـروع كالحصول عليها عن طريق السرقة والقرصنة [3] .
4- صعوبة التجاوب مع حقوق الزبائن : يختلف التقيد بالقوانين من قبل الشركات المعنية من دولة الى أخرى بـالنظر الى الوعي القـانوني في كـل دولـة وأيضـا الجـديـة في تطبيقهـا ، والملاحظ ان التشريعات الاوربية تملك من القواعد القانونية التي تضمن عدم الاحتفاظ بالبيانات الشخصية لمدة تتجاوز الغرض من جمعها وهذا على خلاف التشريعات الأخرى وخصوصا في المنطقة العربية كالقانون الكويتي الذي خلا تماما من تحديد مدة للاحتفاظ بالبيانات الشـخصـية كما خلا من الزام الشركة بمحوها فور انتهاء الغرض من معالجتها [4].
5- مما تقدم يمكننا القول ، ان الخطر يتحقق منذ اللحظة الأولى لقيام الزبون بالادلاء ببياناته الشخصية لدى الشـركة ، ومن ثم يكون الخطر ماسـا بحقه في الدخل بطي النسـيان عندما يزاح السـتار عن بياناته الشخصية القديمة المخزونة التي كانت معروفة لدى الجمهور سابقا ، وهو ما دعا اصحاب الفكر القانوني والباحثين فيه إلى البحث عن حلول لهذه المشـكلة لحماية خصـوصـية الأشـخاص،

---

[1] د. عبد الهادي فوزي العوضـي ، الحق في الدخول في طي النسيان على شبكة الانترنت ، الطبعة الأولى ، دار النهضـة العربية ، القاهرة ، 2013 ، ص81 .

[2] حنين جميل أبو حسـين ، الاطار القانوني لخدمات الامن السـيبراني ، رسـالة ماجسـتير مقدمة الى كلية الحقوق ، جامعة الشرق الأوسط ، المملكة الأردنية الهاشمية ،2021 ، 38 .

[3] Guillaume Desgens-Pasanau,op,cit,p662 .

[4] انظر نص المادة 36 من قانون المعاملات الالكترونية الكويتي رقم 20 لسنة 2014 .

ووجد ضـــالته في مفهوم" الحق في النســيان" في البيئة الرقمية، باعتباره أحد الحقوق المرتبطة بحرمة الحياة الخاصـــة للإنســـان. ولهذا نص المشـــرع المصـــري (م 2 م قانون حماية البيانات الشخصية النافذ) على حق الشخص المعني بالبيانات في محو بياناته الشخصية، مطلقا على الحق المذكور الحق في المحو تسمية "الحق في النسيان" ، اما في نطاق الفقه القانوني فقد أضيفت للحق المذكور تسـميات عدة وان اشـتركت جميعها في المعنى مطلقة عليه مسـمى الحق في الدخول في طي النسيان، أو الحق في النسيان الرقمي [1]. ويقصد بهذا الحق (أن لكل شخص الحق في حذف البيانات الشخصية المحفوظة لدى المعالج أو المتحكم أو الحائز نهائياً عند إلغاء أو مغادرة الخدمة أو التطبيق، وعدم الاحتفاظ بنسـخ منها لأى سـبب كان، بما يتضـمنه ذلك من إزالة الروابط التي تؤدي إلى معلومـات عنـه على الانترنـت (محركـات البحـث، مواقع إلكترونيـة، مواقع التواصـــل الاجتماعي...)[2]، كما يعنى أيضاً التزام المسؤولون عن معالجة البيانات الشخصية أو حفظها بعدم حفظ تلك البيانات لمدة تتجاوز الغاية التي جمعت من أجلها)[3] ، وقد حظى هذا الحق باهتمام بالغ فى أوروبا، وخاصـة بعد صـدور حكم محكمة العدل الأوروبية رقم 12 C-131 / الصـادر بتاريخ 13 مايو 2014 ضد محرك البحث " ("Google)[4]، الذى أوصى المشرع الأوروبي بضرورة وضـع ضمانات لحماية هذا الحق، وقد استجاب المشرع لذلك حيث اعترف صراحة بهذا الحق في المـادة 17 من اللائحـة الأوروبيـة لحمـايـة البيـانـات، حيث تنص في الفقرة الأولى على أن يكون لصـاحب البيانات الحق فى أن يحصـل من المتحكم على محو البيانات الشـخصـية المتعلقة به دون تأخير لا مبرر له، ويجب على المتحكم أن يحذف البيانات الشخصية دون تأخير.

وبناءً على ذلك تمكن المسـتخدم الأوروبي من مطالبة شـركات الانترنت بحقه في محو بياناته الشـخصـية واحترام حقه في الدخول في طي النسيان الرقمي [5].

---

[1] د. عبد الهادي فوزي العوضـي ، الحق في الدخول في طي النسـيان على شـبكة الانترنت ، دار النهضـة العربية ، ط1 ، 2014 ، ص36.

[2] د. معاذ سليمان الملا ، مصدر سابق ، ص 119 .

[3] عرفت اللجنة الوطنية للمعلومات في فرنسـا ، الحق في النسيان الرقمي (بانه الحق الذي يخول صاحبه مكنة السيطرة من حيث الزمان على بيانته الشـخصـية ، بغية الحصول على حذفها او محوها عندما يرغب في ذلك)، منقول من د. عبد الهادي فوزي العوضي ، المصدر نفسه ، ص39.

[4] صـدر حكم محكمة العدل التابعة للاتحاد الأوروبي رقم 12 C-131 / في 13 مايو)آيار(2014 ، بشـأن قضية اشتهرت بقضـية ماريو كوستيغا ضد محرك البحث جوجل Google أسبانيا وجوجل الرئيسي الكائن في الولايات المتحدة الأمريكي، حيث قضـــت المحكمة بحق مســتخدمي الانترنت في مطالبة محركات البحث مثل Google بإزالة نتائج طلبات البحث التي تتعلق بالبيانات الشخصية، متى كانت الروابط المعنية "غير كافية أو غير ذات صلة أو لم تعد ذات صلة بموضوع البحث أو مبالغًا فيها"، حتى ولو كان المحتوى صحيحاً ومنشوراً بشكل قانوني طالما رغب الشخص في نسيانها. وقد استندت المحكمة في قرارها إلى الأحكام الواردة في التوجيه الأوروبي رقم 95 / 46 بشـأن حماية معالجة البيانات الشـخصـية ونقلها، وأيضـاً الاتفاقية الأوروبية لحقوق الانسـان الصـادرة عام 1950 . لمزيد من التفصـيل راجع: الصـالحين محمد العيش، تعليق حول حكم محكمة العدل الأوروبية الصادر في 13 مايو 2014 بشأن الحق في اعتبار بعض الوقائع في طي النسيان، بحث منشور بمجلة معهد دبي القضائي، العدد 5، 3 فبراير 2015 ، ص 169 وما بعدها؛ د. معاذ سليمان الما: فكرة الحق في الدخول في طي النسـيان الرقمي في التشـريعات الجزائية الإلكترونية الحديثة دراسـة مقارنة بين التشـريع العقابي الفرنسـي والتشـريع الجزائي الكويتي، بحث منشـور في مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السـنوي الدولي الخامس، 9 - 10 مايو 2018 ، ملحق خاص، العدد 3، الجزء الأول، مايو 2018 م، ص 117 وما بعدها.

[5] يُشـار في هذا الصـدد، إلى قيام شـركة Google بتضـمين سـياسـتها لتقرير الشـفافية إعلام المسـتخدمين لمحركها بتأثير قانون الخصـــوصـــية الأوروبي في نتائج بحث Google ، وبيان "طلبات حذف المحتوى بموجب قانون الخصـــوصـــية الأوروبى"، وطلبات إزالة عناوين URL من بحث Google للحفاظ على الخصوصية، وذلك على موقعها التالي :

ولكن ينبغي علينا التطرق لا سباب تطبيق الحق في النسيان لاهميته بالنسبة للزبائن ، وخطورته للشركات كونه يمثل رأس مال ورصـيد مهم في هذا المجال ، وان كان لم يحدد المشـرع المصـري الحالات التي ينطبق فيها الحق في المحو أو ما يطلق عليه الحق في النسـيان ، وهو ما تحوط له المشـرع الأوروبي في اللائحة الأوروبية، حيث تضمنت المادة 17 منه أحكام واضحة لتنظيم هذا الحق، واشترطت لتطبيق الحق في النسيان ضرورة توافر أحد الأسباب التالية :

1- لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها من أجلها
2- قيام صاحب البيانات بسحب الموافقة التي تستند إليها المعالجة وفقًا للفقرة الأولى من المادة 6، أو الفقرة الأولى من المادة 9، وحيث لا يوجد أساس قانوني آخر للمعالجة؛
3- اعتراض صـاحب البيانات على المعالجة وفقًا للمادة 21 / 1 ولا توجد أسـباب مشـروعة تبرر المعالجة، أو اعتراضه على المعالجة وفقاً للمادة 21 / 2؛
4- - إذا جرى معالجة البيانات الشخصية بشكل غير قانوني
5- - يجب محو البيانـات الشـخصـيـة للوفاء بـالتزام قـانوني في قانون الاتحاد الأوروبي أو الدول الأعضـاء يخضـع له المتحكم؛ تم جمع البيانات الشـخصـية بخصـوص عرض خدمات مجتمع المعلومات المشار إليها في المادة 8/ 1.

وفي حالة قيام المتحكم بإتاحة البيانات الشخصية للشركات، وكان ملزماً بمحو البيانات الشخصية، يجب عليه، مع مراعاة التكنولوجيا المتاحة وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير التقنية، لإبلاغ المتحكمين في معالجة البيانات الشـخصـية بأن صـاحب البيانات قد طلب محو أي روابط لديهم أو نُسخ لهذه البيانات الشخصية [1].

بالمقابل فأنه ينحصـر مجال تطبيق الحق في النسـيان في البيئة الرقمية فيما يتعلق بالآثار الإلكترونية أو الذكريات الرقمية، وهى كل البيانات والمعلومات المتعلقة بالشـخص ونشـاطه حال اسـتخدامه لنشـاط معلوماتي أو وسيلة الكترونية أياً كان نوعها (شركات التحويل المالي - محركات بحث – مدونات - مواقع التجارة الالكترونية.. وغيرها) يكون من شـأنها أن تسـاهم في تحديد هويته الرقمية، كما يعتبر من الآثار الرقمية أراء الشخص ومساهماته على الانترنت مهما كان نوعها. وحديثاً، قضت محكمة العدل الأوروبية، بتاريخ 24 سبتمبر 2019 ، بأنه إذا كان يتوجب على شـركة " Google " سـحب روابط بطلب من هيأة تنظيميـة أو محكمـة في دولـة بـالاتحـاد الأوروبي من جميع نسـخ مواقعهـا الأوروبيـة، إلا أن "الحق في النسـيان" عبر الإنترنت يتوقف عند هذا الحد، ومن ثم فهى غير مطالبة بتطبيق هذا الحق على محركات البحث التابعة لها خارج أوروبا.[2]

وأشـارت المحكمة إلى أن قانون الاتحاد الأوروبي لا يشـترط على مشـغلي محركات البحث على غرار Google القيام بعملية سـحب روابط كهذه في جميع نسـخ محرك البحث التابع لها. لكنها شـددت على أن سحب الروابط من المواقع الأوروبية يجب أن يتضمن إجراءات "تثني جدياً" مستخدم الإنترنت الأوروبي عن التمكن من الالتفاف على "حق النسيان" من خلال الوصـول إلى نتائج لا قيود عليها عبر محرك بحث

https//:transparencyreport.google.com/eu-privacy/overview?hl=ar&hl=es

[1] انظر نص المادة 17 /ثانيا من اللائحة الاوربية لحماية البيانات الشخصية (GDPR)

[2] Google LLC , successor to Google lnc . v Commission nationale de l,informatique et des libertes (CNIL) and others , Case C- 507/17, 10 January 2019 , available at : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? Uri =CELEX : 62017CC0507&from=en.

في نطاق خارج الاتحاد الأوروبي، ويتطلب ذلك فرض "حجب جغرافي"، وهو أمر تشير جوجل إلى أنها تطبقه بفعالية في أوروبا.

ويرى الباحث بضرورة تحديد مدة معينة يتعين تصحيح البيانات خلالها أو حذفها حتى لا تكون الشركات تحت رحمة الزبون متى ما أراد ممارسة الحق في النسيان ، وأيضا تطبيقا لمبدأ استقرار المعاملات .

الفرع الثاني

الالتزام بالخصوصية في حالة المنع

الأساس في البيانات الشخصية هو ضرورة الالتزام بخصوصيتها وعدم الإفصاح عنها او نقلها الى الغير، وهذا ما نصت عليه جل التشريعات المقارنة ، ومما يعني انه تلتزم الشركات المتعاملة مع البيانات الشخصية للزبائن بعدم القيام باي عمل من شانه يخالف هذا المبدأ ، الا اذا سمح الزبون بذلك صراحة ، ولعل من ابرز التصرفات التي تخالف خصوصية البيانات الشخصية هي :

أولا : الالتزام بتأمين البيانات الشخصية : ان استخدام التقنية الرقمية في حفظ البيانات الشخصية على شكل قواعد بيانات وارتباط هذه القواعد بشبكة الانترنت ، أدى الى تعاظم خطر الدخول اليها عن طريق الشبكة من قبل افراد غير مأذون لهم الدخول اليها او الاطلاع عليها ، مما يشكل انتهاكا لخصوصية أصحاب الشأن فيها [1] .

ومن اجل تحقيق هذا الالتزام فرضت اللائحة الاوربية (GDPR) الالتزام بالتأمين اذ انها نصت المادة 32 منها ((على انه مع الاخذ في الاعتبار اتباع احدث وسائل المعالجة وتكاليف تنفيذها ، وطبيعة ونطاق واغراض المعالجة ، وكذلك المخاطر على حقوق وحريات الأشخاص الطبيعيين من حيث احتمال وقوعها وشدتها ، يجب على المسؤول عن المعالجة (المراقب) ومعالج البيانات الشخصية من الباطن ، تنفيذ التدابير التقنية والتنظيمية المناسبة لضمان مستوى من الامن يتناسب مع المخاطر ومن هذه التدابير مايلي[2]

1- الاسم المستعار وتشفير البيانات الشخصية [3] .
2- القدرة على ضمان استمرار سرية ونزاهة وتوافر مرونة أنظمة وخدمات المعالجة .

---

[1] د. محمد سامي عبد الصادق ، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية ، دار النهضة العربية ، 2016 ، ص7.

[2] ومن الإجراءات التأمينية الأخرى : وضع كلمة سر على قواعد البيانات بحيث لا يتم السماح بالدخول الى هذه القواعد الا لبعض الأشخاص المأذون لهم بذلك والمسؤولين عن معالجة البيانات ، لمزيد من التفاصيل حول ذلك انظر ، د. خالد ممدوح إبراهيم ، أمن الجريمة الالكترونية ، الدار الجامعية ، الإسكندرية ، 2008 ، ص39 .

[3] ويمكن تعريفه بأنه : مجموعة تقنيات تسمح بحماية المعلومات عن طريق رمز سري ، وهو طريقة تسمح بتشفير المعلومات المرسلة بواسطة مفتاح خاص او عام ، ثم فك تشفيرها بعد ذلك ، مما يعني منع الأشخاص غير المصرح لهم من الوصول الى الرسالة . انظر د. خالد ممدوح إبراهيم ، المصدر نفسه ، ص43 .

3- القدرة على استعادة توافر البيانات الشخصية والوصول اليها في الوقت المناسب في حالة وقوع حادث مادي او تقني .
4- اجراء الاختبار وتحليل وتقييم فعالية التدابير التقنية والتنظيمية لضمان امن المعالجة بصورة منتظمة.

وعند تقييم المستوى المناسب من الامن يجب ان تؤخذ في الاعتبار بصفة خاصة المخاطر التي تنطوي على حماية البيانات ، وخاصة ما كان منها ناجما عن التدمير او الفقدان او التغيير او الكشف غير المأذون به عن البيانات الشخصية المرسلة او المخزونة او المعالجة بطريقة أخرى او الوصول غير المأذون به الى هذه البيانات بطريق الخطأ او بصورة غير مشروعة .

ويجب ان يتخذ المسؤول عن المعالجة ومعالج البيانات من الباطن تدابير لضمان ان أي شخص طبيعي يعمل تحت سلطة أي واحد منهما وله حق الوصول الى البيانات الشخصية لا يقوم بمعالجتها الا بناء على تعليمات المراقب (المتحكم) مالم يكن ذلك مطلوبا بموجب قانون الاتحاد او الدولة العضو)) .

ويستفاد من هذا النص ما يلي :

أ -إن الالتزام بتأمين البيانات الشخصية يقتضي بطبيعته أن يقوم المسؤول عن معالجة البيانات الشخصية ومعالج البيانات الشخصية من الباطن باتخاذ كل الاجراءات التقنية اللازمة لايجاد مستوى حماية ملائم لهذه البيانات من حيث طبيعتها والاخطار التي من المحتمل أن تتعرض لها والتقنيات المتاحة في مجال حمايتها[1] ؛ الامر الذي يتطلب منهما-في معرض تنفيذ هذه الاجراءات- ان يكونا مزودين بتقنيات حماية ذات مستوى متقدم، وأن يكون لديهما فريق تقني مدرب لحماية البيانات وقادر على اتخاذ الاجراءات المناسبة فوراً في حالة حدوث أي مشكلات يمكن ان تصيب قواعد البيانات ، وان يكونا مواكبين للتطورات التقنية في مجال حماية البيانات ، لان هذه المسألة امر متطور من آن لاخر ، فالتقنية التي تصلح اليوم لحماية البيانات قد لا تصلح بعد عدة شهور ، نظرا لظهور مخاطر جديدة يمكن ان تصيب قواعد البيانات ولا تستطيع التقنية القديمة ان تدفعها [2].

ب – ان تأمين البيانات لا يقتصر على تأمينها فقط من دخول الغير للاطلاع عليها ، وانما يمتد الى تأمينها من أي خطر يهدد وجودها كتدميرها نتيجة حادث فني او فقدها او العبث بها او تغييرها او تشويهها [3].

وتاكيدا لذلك اكدت محكمة النقض الفرنسية في حكمها الصادر في 30 أكتوبر 2001 على التزام المسؤول عن إجراءات معالجة البيانات الشخصية بتأمين هذه البيانات بالوسائل الملائمة والتي من شأنها منع الأشخاص غير المصرح لهم بالولوج اليها او الاطلاع على مضمونها [4].

اما المشرع المصري فقد اخذ بالالتزام بتأمين البيانات والمعلومات في قانون مكافحة جرائم تقنية المعلومات ونص عليه باعتباره واحدا من الالتزامات والواجبات الملقاة على عاتق مقدم الخدمات بالبند 3

---

[1] Cynthia CHASSIGNEUX, La protection des données personnelles, en France , op , cit, p , 7

[2] انظر تقرير الأمم المتحدة ، اللجنة الاقتصادية والاجتماعية لغربي اسيا (الاسكوا) عن بناء الثقة بالخدمات الالكترونية في منطقة الاسكوا ، 2009 ، ص3 ، E/ESCWA/ICTD/2009/4

[3] Cynthia CHASSIGNEUX, La protection des données personnelles, en France , op , cit, p , 18.

[4] Cass. Crim., 30 octobre 2001, N° de pourvoi : 99-82136, Disponible sur www.legifrance.gouv.fr, Le : 16/03/2020

من الفقرة (أولا) من المادة 2 منه " يلتزم مقدمو الخدمات بتأمين البيانات والمعلومات بما يحافظ على سريتها ، وعدم اختراقها او تلفها " .

وان المشرع المصري اعتبر هذا الالتزام من الالتزامات المفروضة على عاتق المتحكم بموجب المادة (4) من قانون حماية البيانات الشخصية المصري ، في البند (6) من المادة أعلاه " يلتزم المتحكم باتخاذ كافة الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظا على سريتها ، وعدم اختراقها او اتلافها او تغييرها او العبث بها قبل أي اجراء غير مشروع " ، كما أورد المشرع المصري الالتزام ذاته في جملة الالتزامات الملقاة على عاتق المعالج في المادة (5) من القانون ذاته ، في البند (7) من المادة آنفة الذكر " يلتزم معالج البيانات الشخصية بحماية وتأمين عملية المعالجة والوسائط والأجهزة الالكترونية المستخدمة في ذلك وما عليها من بيانات ".

ثانيا : الالتزام بعدم افشاء البيانات الشخصية : يقع على عاتق الشركة التزاما أساسيا بعدم افشاء بيانات الزبائن الشخصية الى الشركات الأخرى ، اذا كان من شأنه ان يهدد اعتبار الزبون فيها او حياته الخاصة ، وبمفهوم المخالفة ان الشركة مسموح لها افشاء البيانات الشخصية التي لا يكون في افشائها أي تهديد لكرامة واعتبار الزبون او لحياته الخاصة ، وهو امر يعود تقديره للقضاء في كل حالة على حدة ، لانهل ايمكن مسبقا تحديد البيانات التي يمثل افشاؤها للغير تهديدا للحياة الخاصة او الكرامة من عدمه ، فلا يوجد معيار ثابت لذلك ، بل هي أمور تختلف من شخص لاخر ، وباختلاف الأزمنة والامكنة [1].

وذكر المشرع المصري الالتزام بعدم افشاء البيانات الشخصية من جملة الالتزامات والواجبات الملقاة على عاتق مقدم الخدمات بموجب قانون مكافحة جرائم تقنية المعلومات ، واورده في البند (2) من الفقرة (أولا) من المادة (2) من القانون المذكور اذ نص على انه " يلتزم مقدمو الخدمات بالمحافظة على سرية البيانات التي تم حفظها وتخزينها ، وعدم افشائها او الإفصاح عنها بغير امر مسبب من احدى الجهات القضائية المختصة ، ويشمل ذلك البيانات الشخصية لاي من مستخدمي خدمته ، او أي بيانات او معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون ، او الأشخاص والجهات التي يتواصلون معها " ، وقد فرض المشرع المصري الالتزام ذاته على عاتق كل من المتحكم والمعالج في قانون حماية البيانات الشخصية اذ نص على انه " يلتزم المتحكم او المعالج القيام بعمل او الامتناع عن عمل يكون من شأنه اتاحة البيانات الشخصية او نتائج المعالجة الا في الأحوال المصرح بها قانونا "[2].
ونلاحظ ان المشرع المصري فيما عدا حالة موافقة الشخص المعني على الكشف عن بيانته الشخصية ، عالج حالات السماح بافشاء البيانات الشخصية او اتاحتها او الإفصاح عنها في قانون حماية البيانات الشخصية بطريقة مختلفة عن قانون مكافحة جرائم تقنية المعلومات ، فجعلها هذا الأخير بناء على امر مسبب من احدى الجهات القضائية المختصة ، في حين تركها لتقديره في قانون حماية البيانات الشخصية .

وعلى الرغم من ان المشرع الأوربي لم ينظم هذا الالتزام بشكل مستقل ، الا ان بعض التشريعات الاوربية نصت عليه وفصلت احكامه كما هو الحال في فرنسا اذ اشارت اليه المادة (22) من قانون العقوبات الفرنسي .

ثالثا : احترام ضوابط حركة البيانات الشخصية عبر الحدود : عالجت المادة 44 وكذلك المواد (45-46) موضوع نقل البيانات الشخصية لاشخاص ينتمون لدول الاتحاد الأوربي الى دولة خارج هذا الاتحاد او

---

[1] د. سامح عبد الواحد التهامي ، ضوابط معالجة البيانات الشخصية ، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي ، مجلة كلية القانون الكويتية ، العدد التاسع ، السنة الثالثة ، 2015، ص422 .

[2] المادة 4 البند (5) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

منظمة خارج دول الاتحاد الأوربي ، سواء تمت معالجة البيانات ومن ثم نقلها او تم جمعها ونقلها في دولة خارج اوربا ، ويندرج ضمن هذه المواد الشروط الأولية لتصح عملية النقل [1]، حيث تبين اللائحة ان النقل يجب ان يتم لدولة تصل فيها قوانين ومستوى حماية البيانات الى المستوى المعمول به في دول الاتحاد الأوربي ، مما يضمن سلامة هذه البيانات ومشروعية العمل بها ، وتتابع المادة 45 لتوضح ان نقل البيانات وجمعها في دولة خارجية يجب ان يسمح به في حال اعتبرت المفوضية الاوربية هذه الدولة او الشركة التي تقع ضمن هذه الدولة لديها المعايير الكافية لحفظ البيانات بشكل آمن وضمن معايير الاتحاد الأوربي ، وادرجت المادة في فقرتها الثانية هذه المعايير ابتداء من كون هذه الدولة تحترم حقوق الانسان ، ولديها القدر الكافي من الحريات ، وكذلك وجود تشريعات متعلقة بحماية البيانات ، وتابعت المادة في الفقرة (2) توصيف هذه المعايير بالحديث عن وجوب وجود هيأة اشراف في هذه الدولة تتولى مهمة تقييم ومراقبة معالجة البيانات ، وتأتي الفقرة الثالثة من المادة نفسها لتشير الى دور المفوضية الاوربية في تصنيف الدول خارج الاتحاد الأوربي وفقا للمعايير المذكورة انفا ، وهذا التصنيف يبين فيما اذا كانت الدولة مؤهلة لتتم عملية نقل البيانات اليها ، وأضافت الفقرة نفسها ما يفيد بأن هذا التصنيف لابد ان يتم بشكل دوري نظرا للتغيرات التي قد تطرأ على الدول من حيث استيفائها للمعايير المطلوبة ، وعليه فأن هذا التصنيف يجب مراجعته كل اربع سنوات على الأقل كما بينا ذلك مسبقا .

ومع ذلك فانه عندما تقوم المفوضية الاوربية بإلغاء او تعديل او تعليق قرار الكفاية المعتمد ، يجوز مع ذلك للشركة نقل البيانات الشخصية او ان تأذن بنقل البيانات المحولة أصلا ، لدولة ليست في الاتحاد الأوربي اذا كانت الضمانات المناسبة لحماية البيانات الشخصية متوفرة في صك ملزم قانونا ، او اذا كان الشخص المسؤول يعتقد وبعد تقييم جميع ظروف النقل ان هناك ضمانات مناسبة لحماية البيانات الشخصية[2] .

وفي مصر فقد حظر المشرع المصري اجراء عمليات نقل البيانات الشخصية التي تم جمعها او تجهيزها للمعالجة الى دولة اجنبية او تخزينها او مشاركتها الا بتوفر مستوى من الحماية في هذه الدولة لايقل عن المستوى المنصوص عليه قانونا ، وبترخيص او تصريح من المركز [3] .

كما أوضحت الفقرة الثانية من المادة ذاتها ان " اللائحة التنفيذية لقانون حماية البيانات الشخصية تحدد السياسات والمعايير والضوابط والقواعد اللازمة لنقل او تخزين او مشاركة او معالجة او اتاحة البيانات الشخصية عبر الحدود وحمايتها ".

ومع ذلك فان المشرع المصري أورد استثناءات من حكم المادة أعلاه ، سمح فيها بنقل او مشاركة او تداول او معالجة البيانات الشخصية الى دولة لا يتوفر فيها مستوى الحماية المنصوص عليه قانونا وهو ما بيناه سابقا .

وقدر تعلق الامر في خصوصية موضوع التحولات المالية وكونها الأكثر تعلقا بموضوع الدراسة نلاحظ ان المشرع المصري استثناها من القيد المفروض على حرية نقل البيانات الى دولة أخرى ، وهو ما

---

[1] Cynthia CHASSIGNEUX, La protection des données personnelles, en France , op , cit, p , 8.

[2] Guillaume Desgens-Pasanau,op,cit,p6656.

[3] المادة (14) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 وقد أورد المشرع المصري في المادة (2) من القانون المذكور معنى المركز بكونه مركز حماية البيانات الشخصية .

سنتناوله في الفصل الثالث من هذه الاطروحة في موضوع التعارض بين التحويلات المالية وخصوصية البيانات الشخصية[1].

هذا وقد جاءت الفقرة الأولى من المادة (16) من قانون حماية البيانات الشخصية المصري بحكم خاص مفاده جواز قيام المتحكم او المعالج بحسب الأحوال باتاحة البيانات الشخصية لمتحكم او معالج اخر خارج جمهورية مصر العربية بترخيص من المركز ، متى توفرت الشروط الاتية :

1- اتفاق طبيعة عمل كل من المتحكمين او المعالجين ، او وحدة الغرض الذي يحصلان بموجبه على البيانات الشخصية .
2- توافر المصلحة المشروعة لدى كل من المتحكمين او المعالجين للبيانات الشخصية او لدى الشخص المعني بالبيانات .
3- ان لا يقل مستوى الحماية القانونية والتقنية للبيانات الشخصية لدى المتحكم او المعالج الموجودة بالخارج عن المستوى المتوافر في جمهورية مصر العربية .

كما اشارت الفقرة الثانية من المادة نفسها الى ان اللائحة التنفيذية لقانون حماية البيانات الشخصية هي التي تحدد الاشتراطات والإجراءات والاحتياطات والمعايير والقواعد اللازمة لذلك .

ثالثا : اتلاف البيانات الشخصية : من صور الالتزام بالخصوصية ، التزام الشركة بعدم اتلاف بيانات الزبائن الشخصية ، ويعرف اتلاف البيانات الشخصية بأنه " محو البيانات او البرامج كليا او تدميرها او ان يتم تشويه المعلومة او البرنامج على نحو فيه اتلاف بها يجعلها غير صالحة للاستعمال ".[2] وفي السياق ذاته عرف بأنه (المحو او التشويه الالكتروني للبرامج او المعلومات او البيانات او المحررات الالكترونية كليا او جزئيا على نحو يجعلها غير صالحة للاستعمال)[3] . وعلى ذلك فاتلاف البيانات الشخصية هو الذي يقع على المكونات المعنوية للنظام المعلوماتي ، أي البيانات الشخصية والبرامج . والظاهر ان موضوع هذا الاتلاف هو البيانات المعالجة آليا وكذلك المسار او البيانات او المعلومات المخزونة او المعالجة .اضافة الى الاتلاف او التعطيل او التعديل او الإلغاء غير المشروع وما يترتب على ذلك من نتيجة وهي اتلاف بيانات الزبائن .

ويذهب البعض الى انه لا توجد شروط تتعلق بطبيعة البيانات محل الاتلاف او تبعيتها لجهة معينة او شخص محدد ، بل الامر عام ويتسع لكافة أنواع البيانات ، وايا كان صاحب الشأن فيها [4] .كما انه لافرق فيما اذا كانت هذه البيانات ذات قيمة اقتصادية حتى تتمتع بالحماية القانونية ام لا ، اذ ان كثيرا من البيانات الشخصية او المعلومات لها أهمية وقيمة كبيرة على الرغم من عدم تمتعها بقيمة اقتصادية ، وذلك لتعلقها بمجالات مهمة في الحياة كالصحة او العدالة على سبيل المثال [5].

وبقي ان نشير الى ان الأفعال السابقة لا تمثل خرق من قبل الشركة الا اذا ارتكبت بطريق الغش ، أي بدون تصريح او بدون حق ، وبالتالي فالانشطة العادية المتضمنة في تصميم شبكات او تطبيقات شائعة للتشغيل او لممارسات التجارية ، مثال ذلك تلك التي تطابق محاولات اختبار او حماية امن نظام ،

---

[1] د. زكريا يونس احمد ، اثبات عملية التحويل المصرفي الالكتروني وحجيتها ، بحث منشور في مجلة كلية الحقوق جامعة تكريت ، السنة السادسة ، المجلد السادس ، العدد (2)الجزء (2) 2022 ، ص125 .

[2] د. ايمن عبد الله فكري ، مصدر سابق ، ص153 .

[3] د. عمار عباس الحسيني ، جريمة الاتلاف المعلوماتي ، دراسة قانونية مقارنة ، منشورات زين الحقوقية ، ط1، بيروت ، لبنان ، 2019، ص23.

[4] د. عمار عباس الحسيني ، المصدر نفسه ، ص152 .

[5] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الالي الاقتصادية ، مصدر سابق ، ص196 .

والمصرح بها من قبل صاحب البيانات او الجهة المسؤولة قانونا بالتالي تعتبر أنشطة مشروعة ولا تمثل اعتداء على هذه البيانات .

رابعا : الالتزام بالاخطار في حال معالجة البيانات الشخصية : لم يضع المشرع المصري أي التزام على الشركة بالاخطار في حالة المعالجة ، واكتفى بالنص على الالتزام بالاخطار في حالة خرق وانتهاك للبيانات الشخصية [1] . وفي المقابل قد سبق المشرع الأوربي القانون المصري بتنظيمه لهذا الامر [2] في حين تذهب بعض التشريعات الاوربية الى أن معالجة البيانات الشخصية للزبون لا يمكن القيام بها من جانب الشركة الا بعد اخطار صاحبها [3]، وهذا الاخطار يتعين ان يكون متضمنا امرين :

1- اخطاره بمعالجة بيانته الشخصية التي يتعين ان تتم في اطار من الشفافية العالية والأمانة واحترام كرامة الانسان ، بحيث لا يجوز القيام بها دون اخطار صاحب البيانات والحصول على اذن كتابي مسبق منه في بعض الحالات التي نص عليها القانون
2- اخطاره بالغرض من المعالجة الذي يجب ان يكون مشروعا .

ويتعين ان يتسم الاخطار بالشفافية ، بحيث يتعين على القائم بالمعالجة عند جمع البيانات الشخصية لاي فرد إبلاغه بكافة المعلومات التي تتعلق بجمع بيانته ومعالجتها ، وبصفة خاصة بالغرض من جمعها ومن الشخص الذي سيحص عليها حتى يكون على علم مسبق بذلك [4].

والالتزام باخطار الزبون صاحب البيانات بمعالجة بيانته ، وبالغرض منها يتفرع عنه امر اخر الا وهو ضرورة قيام القائم بالمعالجة قبل شروعه فيها أخطاره بالإجراءات المتبعة لحماية البيانات ، على ان تشمل هذه الإجراءات تحديد هوية المسؤول عن المعالجة وطبيعة البيانات والغرض من معالجتها وطرق ومواقع المعالجة وكل المعلومات الضرورية لضمان معالجة آمنة للبيانات. كما يتعين عليه اخطاره باي فشل لبيانات غير دقيقة عنه [5].

وفيما يتعلق بشكل الاخطار ، يتعين على الشركة قبل الشروع والبدء في عملية المعالجة اخطار او اعلام جميع الافراد الذين ستجمع عنهم بياناتهم مسبقا وقبل التاريخ المحدد للمعالجة ، بخطاب ثابت التاريخ ، وفي أي وسيلة تترك اثرا كتابيا في اجل لا يقل عن مدة معينة حددتها بعض التشريعات بشهر [6].

وفي النهاية يجب ملاحظة ان الالتزام بأخطار صاحب البيانات معالجة بيانته ، لا يقتصر فقط عند بدء المعالجة بل يتعين على الشركة اخطاره والمستفيد منها بكل تغيير ادخل على البيانات التي سبق ان حصل عليها .

---

[1] انظر نص المادة 7 من قانون حماية البيانات الشخصية المصري .

[2] انظر نص المادة 19 من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016.

[3] انظر نص المادة 32 من قانون المعلوماتية والحريات الفرنسي رقم (78) لسنة 1978 والمعدل باحكام القانون الصادر في (7) أكتوبر 2016 .

[4] Cynthia CHASSIGNEUX, La protection des données personnelles, en France , op , cit, p , 33.

[5] د. عمرو طه بدوي ، مصدر سابق ، ص167 .

[6] راجع نص الفصل الحادي والثلاثون من قانون حماية المعطيات الشخصية التونسي رقم 63 لسنة 2004.

خامسا : الالتزام بالحصول على الاذن المسبق قبل المعالجة : هناك نوعية من البيانات الشخصية التي تطلبت بعض التشريعات قبل القيام بمعالجتها الحصول على اذن مسبق من صاحبها او من ينوب عنه[1] . ونحيل الكلام في شروط القبول وصحته الى ما تناولناه مسبقا في الفصل الأول من هذه الاطروحة.

المبحث الثاني

وسائل حماية البيانات الشخصية

لايكفي تحديد التزامات الشركة تجاه صاحب البيانات للقول باضفاء الحماية القانونية لها ، وانما لابد من ان تكون هناك ضمانات حقيقية لمنع الاعتداء عليها من قبل الشركات والأشخاص ، وتتمثل هذه الضمانات في توفير وسائل انفاذ للقانون الناظم للحماية باعتبارها الضمانة الحقيقية ، ولكن بالمقابل فان هناك ضعف واضح فيها وخصوصا في العراق وبعض التشريعات المقارنة وهو ما سنتناوله في هذا المبحث من خلال المطلب الأول وسائل انفاذ القانون ، والثاني ضعف الضمانات القانونية ، وكالاتي .

المطلب الأول

وسائل انفاذ القانون الناظم لحماية البيانات الشخصية

يكاد يكون قانون حماية البيانات الشخصية هو التجربة التشريعية الأولى في نطاق خصوصية البيانات الشخصية في مصر، وبما أنه في مهده، فمن المتوقع أن يشهد تطبيق هذا القانون العديد من التحديات، خاصة مع استحداثه لمفاهيم وأدوار جديدة على سوق البيانات المصري.

ومن بين هذه التحديات هو تناول رؤية المشرع ذاته لدور الادوات التنفيذية للقانون، فالقانون الجديد قد سار على نهج التشريعات المقارنة بأن استحدث سلطة رقابية في صورة هيأة عامة تقوم على الاشراف على تطبيق القانون ومنحها في سبيل ذلك العديد من الصلاحيات. ولضمان إنفاذ أكثر فعالية فقد نص كذلك على التزام على المتحكمين والمعالجين بتعيين شخص يصبح مسؤولا عن حماية البيانات داخل الشركة نفسها . ولم يغفل المشرع أيضا عن استخدام الاداة العقابية لكفالة الامتثال ألى احكامه، فأفرد الفصل الرابع عشر للجرائم والعقوبات، وقام فيه بمواجهة الاشخاص الخاضعين للقانون بعقوبات أغلبها الغرامات وبعضها الحبس. وسنتناول هذه المسائل على النحو التالي:

الفرع الأول

الاطار المؤسساتي في حماية البيانات الشخصية

عادة ما تتولى مؤسسات قانونية قطاعية في تنفيذ القوانين التي تنظم محور معين ، وهذه المؤسسات بعضها يتمتع بالخبرة والعراقة في هيكلية الإدارة ، لكن فيما يتعلق بالبيانات الشخصية فان اغلب الجهات التي تتولى عملية تنفيذ هذا القانون ومتابعة تنفيذه هي جهات حديثة النشأة نص القانون نفسه على انشائها وعلى المهام التي يضطلع بها وحدود صلاحيته وهي كالاتي :

[1] انظر نص المادة 6 من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016 ، والمادة الثاني من قانون حماية البيانات الشخصية المصري.

أولا : دور مركز حماية البيانات الشخصية : ساير القانون المصري ما جرى عليه العمل في قوانين حماية البيانات الشخصية حول العالم بإنشاء هيأة تشرف على تطبيق هذه القوانين، فنص القانون المصري على إنشاء مركز أطلق عليه تسمية "مركز حماية البيانات الشخصية " ، ونظم عمله في الفصل التاسع، بموجب المواد من (19 إلى 25 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020)، ليكون قبلة المتعاملين في البيانات الشخصية، وهو ما زال في طور التأسيس .وتتنوع الادوار التي خولها القانون للمركز بحيث يمكن القول بأنه سيكون الفاعل الرئيسي في ساحة حماية البيانات المصرية [1]. وبشكل عام فإن المركز سيضطلع بمهام تتعلق برسم السياسة العامة الخاصة بحماية البيانات وتوجيه المتعاملين فيها وإعطائهم التعليمات اللازمة لذلك . وبناء على ذلك فقد خوله القانون إصدار التصاريح والتراخيص والاعتمادات، وهم بمثابة الاجازة التي يتوجب على كل من يستدعي نشاطه العمل في البيانات الشخصية الحصول عليها، ولضمان فعالية أكثر فقد خوله القانون كذلك سلطة توقيع بعض الجزاءات الادارية على من يتخلف عن الامتثال للتعليمات .

ويعد مركز حماية البيانات الشخصية هيأة عامة اقتصادية ومن ثم يخضع لتنظيم قانون الهيئات العامة رقم 61 لسنة 1963 فيما لم يرد في شأنه نص في قانون حماية البياناتً الشخصية (باعتباره قانونا خاصا) ويكون مقره الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، ويتتبع الوزير المختص، وهو وزير الاتصالات وتكنولوجيا المعلومات، وحدد القانون مهمته في حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها (م 19 من القانون .) .

اما في الاتحاد الأوربي فقد إضاف المشرع الأوربي مهمة أخرى للمركز المذكور ، اذ نصت المادة 1/51 من اللائحة الاوروبية على أن من أهداف المركز هو تسهيل تداول البيانات عبر الاتحاد الاوروبي، وهو ما يوجب على السلطة الرقابية - supervisory authority كما اسمتها اللائحة – متابعة المركز في تنفيذ الهدفين معا في الوقت ذاته . ونعتقد في أن هناك دوراً واضحا لمركز حمايةً البيانات حتى يتمكن من القيام بدوره المزمع وفقا لرؤية المشرع .هذا وقد تنوعت الاختصاصات التي يفترض اضطلاع المركز بها، بين ما يمكن تقسيمه إلى أدوار استشارية، وأخرى رقابية،ً مواجها في سبيل ذلك بعض التحديات، وهو ما سنتناوله فيما يلي

أولا : الدور التوجيهي والاستشاري لمركز حماية البيانات الشخصية :أناطت القوانين المنظمة لحماية البيانات الشخصية بالمركز مهمة رسم الملامح العامة لخريطة حماية البيانات الشخصية في مصر، في ظل القانون واللائحة المزعم إصدارها، لذلك نجد المادة (19) تنص على أن المركز هو الجهة المخولة بوضع وتطوير السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية والقيام على تنفيذها. وكذلك يتولى توحيد سياسات وخطط حماية ومعالجة البيانات الشخصية داخل الجمهورية. كما أن المركز سيقوم اعمالا لدوره الارشادي بوضع إطار إرشادي لمدونات السلوك الخاصة بحماية البيانات الشخصية بالجهات المختلفة،

[1] حددت المادة الاولى من قانون حماية البيانات الشخصية الخاصة بالتعريفات المقصود بـ "المركز" بأنه "مركز حماية البيانات الشخصية."

وهو ما يعني أن يقوم المركز إما برسم الخطوط العريضة التي تتبعها الجهات المعنية في وضع مدونات سلوكها، أو أن يضع المركز مدونات سلوك قياسية يقتدى بها مباشرةً [1].

وعملا على اطلاع الجهات المعنية بالبيانات الشخصية بشكل دائم على آخر المستجدات في مجال حماية البياناتً الشخصية ونظم وإجراءات الحماية، خصوصا مع كون هذا المجال في تطور مستمر استجابة للتطورات التكنولوجية، يتولى المركز إصدار الدوريات الخاصة بتحديث إجراءات الحماية بما يتوافق مع أنشطة القطاعات المختلفة، كما ينقل رؤيته وتوجيهاته عبر إصدار توصياته في هذا الصدد[2] .

كذلك وفقا للمادة 19 من القانون ، يعنى المركز بمهمة دعم جهود تطوير كفاءة الاشخاص المفترض بهم القيام على حماية البيانات الشخصية في جميع الجهات الحكومية وغير الحكومية، وهو ما يدلل على دور المركز في تمهيد بيئة امنة للبيانات الشخصية في مصر للتعامل مع القانون الجديد والتغيرات التي يقتضيها ، ويشير القانون في هذا السبيل إلى قيام المركز بتنظيم المؤتمرات وورش العمل والدورات التدريبية والتثقيفية، وإصدار المطبوعات بغرض نشر الوعي والتثقيف للافراد والجهات حول حقوقهم فيما يتعلق بالتعامل على البيانات الشخصية [3]. واجمالا يضطلع مركز حماية البيانات الشخصية بمهمة تقديم جميع أنواع الخبرة والاستشارات المتعلقة بحماية البيانات الشخصية، وهو ما يعضد من دور المركز الاستشاري والتوعوي بالنسبة للاشخاص والمؤسسات على السواء، سواء أكان ذلك في مصر أو في الخارج .

بالاضافة إلى ذلك، يصبح المركز والعاملين فيه بمثابة الخبير في المسائل المتعلقة بالبيانات الشخصية في حالات التحقيق والجهات القضائية، فيتم الاستعانة بهم كخبراء فيً مسائل حماية البينات الشخصية سواء كانت تلك الاجراءات تضطلع بها الجهات الادارية أو المحاكم أو غيرها من جهات القضاء، العادي منها والاداري، كما القضاء العسكري والدستوري [4] .

واتصالا بدوره في رسم السياسات المتعلقة بحماية البيانات الشخصية، يقوم المركز أيضا بالتنسيق والتعاون مع جميع الجهات والاجهزة الحكومية وغير الحكومية في إجراءات حماية البيانات الشخصية، ولا يقتصر هذا الدور على مجرد التواصل والتنسيق التقليدي مع الشركات والمؤسسات التي تتعامل في البيانات؛ المتحكمين أو المعالجين التقليدية .إذ تمتد هذه الفقرة لتشمل التنسيق على مستوى الجهات التي قد يكون لها تأثير على امتثال غيرها من الجهات، والجهات المعنية بمجال حماية البينات الشخصية ذاته وكذلك الاجهزة والجهات الكبرى كانت حكومية أو غير حكومية .

---

[1] يكون للسلطة الرقابية في الانظمة المقارنة اختصاصات تدور بين التحقيق في المخالفات، وسلطة التنظيم، وكذلك سلطة إنزال العقاب؛ أنظر منى الاشقر، محمود جبور، البيانات الشخصية والقوانين العربية: الهم الامني وحقوق الافراد، مصدر سابق ، ص 157 .

[2] د. وسيم شفيق الحجار ، النظام القانوني لوسائل التواصل الاجتماعي ، (واتساب ، فيسبوك،تويتر) ، ط1 ، المركز العربي للبحوث القانونية ، بيروت ، 2017 ، ص173 .

[3] د. دعاء حامد محمد عبد الرحمن ، احكام العلاقة بين مقدمي خدمة الانترنت والمستخدمين بشأن انتهاك حقوق الملكية الفكرية ، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية ، العدد الثالث ، 2018، ص353-354 .

[4] د. هايدي عيسى ، الحاجة لمظلة تشريعية لمارد الدفع الرقمي ، الحاضر والمستقبل ، بحث منشور في مجلة جامعة الشارقة للعلوم القانونية ، المجلد 17 ، 2020 ، ص681 .

وفي السياق نفسه، يعطي القانون للمركز الحق في إبرام الاتفاقيات ومذكرات التفاهم والتنسيق والتعاون وتبادل الخبرات مع الجهات الدولية التي يتصل نشاطها بعمل المركز، وهو ما يعزز خبرات المركز إذا تم تفعيله. فالمركز والقانون من الاساس يعتبران حديثين بعض الشيء إذا ما قورنا بالوضع في الاتحاد الاوربي، لذا فالتعاون مع الجهات الدولية والاستفادة من الخبرات السابقة سيساهم في تطور أسرع للمركز وللممارسات اللازمة في حماية البيانات الشخصية. ذلك مما تؤيده المادة 25ً أيضا، إذ تؤسس للتعاون والتنسيق وتبادل البيانات والمعلومات مع السلطات المختصة في البلاد الاجنبية في سياقات مختلفة [1] .

ثانيا : الدور الرقابي لمركز حماية البيانات الشخصية : إن أحد الدعائم الرئيسية لحماية البيانات الشخصية وفقا للاطار الذي رسمته التشريعات الجديدة هو الدور الرقابي لمركز حماية البيانات الشخصية، فالمركز يفترض فيه أن يكون الجهة التنفيذية للقانون، بما يشمله ذلك من الرقابة على تطبيق القانون وبحث امتثال الجهات المعنية لاحكامه ذلك [2]. وعلى ذلك، فقد انعكست تلك الفلسفة في الدور الرقابي الذي اسكنه القانون المركز، والادوات التي يملكها في سبيل ذلك . وتحدد المادة (19) من القانون أن أحد مهام المركز الهامة، هي القيام على تنفيذ السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات، والتي يضطلع هو ذاته ـ بوضعها. وقد منح القانون المركز اختصاصا عاما للمركز حينما نص في المادة المذكورة على قيام المركز على تطبيق أحكام هذا القانون، كما أن للمركز في هذا الصدد سلطةً إجازة العديد من الانشطة وفقا للقانون، فهو من بيده اعتماد الجهات والافراد الذين يعتزمون تقديم الاستشارات في إجراءات حماية البيانات الشخصية، كما أنه هو الجهة المعنية بإصدار التراخيص والتصاريح والموافقة المتعلقة بحماية البيانات. وبخلاف ذلك فهو الجهة المنوط بها اعتماد مدونات السلوك الخاصة بالجهات المختلفة .

وهذا يعني أن المركز هو المتحكم عملا في مزاولة كافة الانشطة المتعلقة بالبيانات؛ فهو من يرخص للمتحكمين والمعالجين، ومن ناحية أخرى هو من يقرر مدى كفاءة الشخص أو الجهة التي تنوي تقديم الاستشارات في هذا المجال. فهو يراقب مدى انطباق أحكام القانون واللائحة وأحكامه على المعنيين، ومن ثم مدى استحقاقهم للحصول على الترخيص او التصريح اللازم لمزاولة النشاط للمرة الاولى، أو للاستمرار في مباشرته[3]

وتماشيا مع هذه الدور، يقوم المركز أيضا بتلقي الشكاوى والبلاغات المتعلقة بأحكام القانون ، كما يملك فوق ذلك أن يصدر القرارات التي تتراءى له بصدد هذه الشكاوى

---

[1] تنص المادة 25 من قانون حماية البيانات الشخصية على أن: "للمركز بالتنسيق مع السلطات المختصة التعاون مع نظرائه بالبلاد الاجنبية وذلك في إطار اتفاقيات التعاون الدولية والاقليمية والثنائية أو بروتوكولات التعاون المصدق عليهاً أو تطبيقا لمبدأ المعاملة بالمثل بما من شأنه حماية البيانات الشخصية والتحقق من مدى الامتثال للقانون من قبل المتحكمين والمعالجين خارج الجمهورية، ويعمل المركز على تبادل البيانات والمعلومات بما من شأنه أن يكفل حماية البيانات الشخصية وعدم انتهاكها والمساعدة في التحقيق في الانتهاكات والجرائم ذات الصلة وتتبع مرتكبيها. "

[2] د. العربي جنان ، معالجة المعطيات ذات الطابع الشخصي ، الحماية القانونية في التشريع المغربي والمقارن ، ط1، المطبعة الوطنية ، مراكش ، 2010 ، 84 .

[3] حنين جميل أبو حسين ، مصدر سابق ، ص56 .

والبلاغات، وقد دعم القانون ذلك بأن نص صراحة على صلاحية المركز في الرقابة والتفتيش على المخاطبين بأحكام القانون واتخاذ الاجراءات القانونية اللازمة في مواجهتهم [1]

وتتجلى سلطة المركز الرقابية كأوضح ما يكون في الادوات التي منحه القانون إياها، فبخلاف الجزاءات المدنية والجنائية، ينص القانون على مجموعة من الجزاءات الادارية التي يستطيع المركز توقيعها على المخالفين، والتي قد تصل ً إلى حد وقف نشاط الجهة المخالفة تماما، وفي هذا الصدد تقضي المادة (30)أنه في حالة عدم امتثال المخالف للانذار الموجه له بإزالة المخالفة وأسبابها أو أثارها خلال الفترة ً المحددة له بذلك، كان لمجلس إدارة المركز أن يصدر قرارا مسببا بتوقيع الجزاءات التالية

1- الانذار بإيقاف الترخيص أو التصريح أو الاعتماد جزئيا أو ً كليا لمدة محددة .

2- إيقاف الترخيص او التصريح أو الاعتماد جزئيا أو كليا . الايقاف قد يكون مؤقتا، فقد يتم وقف الترخيص أو التصريح أو الاعتماد لمدة معينة من مدتهم الاصلية .

3- سحب الترخيص أو التصريح أو الاعتماد أو إلغاؤه ً جزئيا أو كليا. ونظرا لجسامة جزاء إلغاء الترخيص أو التصريح أو الاعتماد فقط حدد القانون في المادة (29) حالات محددة يقتصر عليها[2]

4- نشر بيان بالمخالفات التي ثبت وقوعها في وسيلة إعلام أو أكثر واسعة الانتشار على نفقة المخالف .

وهذا قد يكبد المخالف خسائر فادحة، فهو يمس مباشرة ً بسمعة المخالف، وتحديدا معايير خصوصية بيانات المستخدمين والزبائن لديه، ومدى أمانته عليها، فحتى وإن كان ذلك ً جزاء تابعا لالغاء الترخيص أو التصريح أو الاعتماد بشكل كلي، فالشركات التي تمارس أكثر من نشاط ليس منها ما سيتضرر مباشرة بهذا الالغاء ستتأثر به سمعتها في العموم، وستتأثر بالتأكيد إذا كانت مؤسسة أو شركة متعددة الجنسيات، حيث سيطال نشر المخالفة من سمعتها في الدول الاخرى التي تمارس فيها نشاطها. ولا حاجة للاشارة لمدى حساسية مسألة خصوصية البيانات ليس فقط بالنسبة للزبائن بل والجهات الحكومية والشركاء[3].

5- إخضاع المتحكم أو المعالج للاشراف الفني للمركز لتأمين حماية البيانات الشخصية على نفقتهما بحسب الاحوال .

ويلاحظ هنا مدى قوة هذه التدابير التي يملكها المركز، فهي قد تصل لحد إيقاف أو سحب الترخيص أو التصريح من المخالف وهو ما قد يعني وقف نشاط الجهة المخالفة بصورة كلية.

---

[1] انظر نص المادة 19 من قانون حماية البيانات الشخصية المصري رقم 20 لسنة 2021 .

[2] تشمل الحالات الواردة في المادة 29 من قانون حماية البيانات الشخصية :
مخالفة شروط الترخيص أو التصريح أو الاعتماد .
عدم سداد رسوم تجديد الترخيص أو التصريح أو الاعتماد .
تكرار عدم الامتثال لقرارات المركز .
التنازل عن الترخيص أو التصريح أو الاعتماد للغير دون موافقة المركز .
صدور حكم بإفلاس المتحكم أو المعالج.

[3] د. اية لبيب محمد عبده عبد الرحمن ، الحماية القانونية للهوية الرقمية ، أطروحة دكتوراه مقدمة الى كلية الحقوق جامعة عين شمس ، 2022 ، ص173 .

وذلك يعضد النظر بأن القانون قد أناط المركز بالتحكم في المعاملات المعنية بالبيانات الشخصية ومصير المخالفين على السواء، وهو ما يتماشى مع الاتجاه الاوربي [1].

بيد أنه من الملاحظ أنه على خلاف معظم القوانين المنظمة لهذا الموضوع، لم يعط القانون المصري المركز سلطة توقيع أية جزاءات مالية على المخالفين للقانون. فالغرامات التي نصت عليها اللائحة الاوربية العامة لحماية البيانات منوط بها الهيئات الرقابية وليس القضاء، وهي قد تصل إلى 20 مليون يورو أو 4 %من إجمالي دخل المخالف . ومن ثم فإن الغرامات المنصوص عليها في هذه القوانين هي غرامات إدارية [2]، الا أن نظيرتها في القانون المصري قد عدها غرامات جنائية، يختص بها القضاء وحده ممثلا في المحكمة الاقتصادية بحسبما نص عليه القانو[3]

يضاف إلى الجزاءات الادارية أن القانون قد منح العاملين بالمركز الذين يصدر بهم قرار من وزير العدل صفة الضبطية القضائية وذلك في إثبات الجرائم التي تقع بالمخالفة لاحكام هذا القانون، لذا يحق لهم التقصي والتحري والحصول على الادلة التي تؤيد إدانة المخالف، بينما يتم مباشرة إجراءات القبض والتفتيش وغيرها من إجراءات التحقيق بمعرفة النيابة العامة.

ثالثا : التحديات التي تواجه عمل مركز حماية البيانات ا لشخصية : لعل من ابرز التحديات التي تواجه مركز حماية البيانات هي

1- وجود الكفاءات اللازمة :سيحتاج الامر إلي تدريبات ودورات مكثفة للحصول على الكفاءات القادرة على تطبيق القانون تقنيا، نظرا لحداثة نصوص القوانين الناظمة لهذا الشأن وخصوصا في المنطقة العربية ، وكذلك تعتبر التطبيقات الدقيقة لحماية البيانات الشخصية جديدة على الكثير من المؤسساتً خاصة تلك التي تمارس نشاطها على المستوى المحلي [4].

أيضا، ومن المحتمل ان يواجه المركز تحديات كبيرة في تغطية احتياجاته من ذوي الكفاءة، ليس فقط على مستوى التمكن التقني، ولكن أيضا على مستوى الاعداد بحيث يستطيع تغطية احتياجات السوق بالكامل، وهي بالعادة اسواق كبيرة، ومستمرة في النمو، خاصة مع توجه الدول إلى تشجيع الانشطة الصغيرة والمتوسطة، وهو ما يعني بالتبعية زيادة المؤسسات المتعاملة في البيانات الشخصية. يدعم ذلك أن القانون يوجب على جميع المتعاملين في البيانات الشخصية الالتزام بأحكامه، بصرف النظر عن حجم نشاطهم. ويتضح ذلك بشدة في الالتزام بالحصول على التراخيص والتصاريح، والذي يعتبره القانون التزاما عاما يوقع على كل من ينصب نشاطه على التعامل في البيانات، أو بتعبير أدق كل من يقع تحت تعريف المتحكم أو المعالج، وهو ما يشمل كل المتعاملين في البيانات تقريبا وذلك لعموم التعريفين [5].

---

[1] د. احمد رجب سيد صميدة ، التنظيم القانوني للحق في الخصوصية ، (المسكن،الاتصالات الخاصة ، البيانات الشخصية) ، ط1، دار النهضة العربية ، القاهرة، 2022 ، ص 632 .

[2] انظر نص المادة (5/83) من اللائحة الاوربية العامة لحماية البيانات الشخصية النافذة .

[3] انظر نص المادة 5 من قانون حماية البيانات الشخصية المصري النافذ .

[4] د. احمد رجب سيد صميدة ، المصدر السابق ، ص 679.

[5] د. احمد رجب سيد صميدة ، المصدر نفسه ، 684 .

ومن التحديات التي تواجه المركز أيضا مشكلة حث الشركات والمؤسسات على الامتثال لاحكامه دون التمادي والمبالغة في استخدام الجزاءات الادارية التي خوله القانون إياها، كما أن الندرة في المتخصصين بهذا المجال ستنعكس أيضا على التزام الشركات والمؤسسات، خاصة وأن هناك البعض منها لا يمتلك بالضرورة القدرة على الوفاء بالاعباء المالية لقانون حماية البيانات، وفي مقدمتها الشركات الصغيرة ، ومن الضروري هنا الاستعانة بالكفاءة التقنية ضمن تشكيل وإدارة المركز لضمان فاعلية تطبيق احكام القانون ولائحته التنفيذية .

2- موارد المركز :في سياق آخر، صمت القانون عن الامكانيات التي يتوجب توفيرها للمركز ليتمكن من ممارسة عمله، ويفترض هنا أن المركز سيتكفل بتدبير احتياجاته المالية باعتباره هيئة اقتصادية كما نص القانون، إلا أن الاخير لم يحدد الوضع بالنسبة لميزانية المركز، وما إذا كانت مستقلة، أم تابعة لوزارة الاتصالات. بيد أنه بالرجوع لقانون الهيئات العامة المصري [1] ، نجد أن الاصل في الهيئات العامة أن يكون لها ميزانية خاصة يصدق عليها رئيس مجلس إدارتها ويتم إقرارها بواسطة الجهة الادارية المختصة، وهي وزارة الاتصالات في هذه الحالة. ولما كان وزير الاتصالات هو نفسه رئيس مجلس إدارة المركز، فيصبح في يده وضع الميزانية وإقرارها[2].

وبالنسبة للاتحاد الاوربي، فإن السلطات الرقابية يفترض أن يكون لها ميزانية مستقلة [3] ، كما يفترض بالدول أن توفر للسلطات الرقابية فيها الموارد المالية والبشرية، والبنية، التحتية اللازمة لاضطلاع السلطة بدورها.

3- استقلال المركز : حرصت اللائحة الاوربية على إنفاذ مبدأ الاستقلال فيما يتعلق بالجهات المنوطة بالرقابة على حماية البيانات (مسؤولً حماية البيانات والهيئة الرقابية، ويفترض وفقا للائحة الاتحاد الاوربي أن تتمتع السلطة الرقابية باستقلال تام في ممارسة نشاطها، وأن يراعي ذلك في تشكيلها وكذلك في مواردها)[4] .

وفي المقابل، لم يسلك القانون المصري السبيل نفسه، ونجد مظاهر ذلك واضحة للعيان في تشكيل مركز حماية البيانات الشخصية، إذ يترأس المركز وزير الاتصالات نفسه، ويشمل مجلس إدارته عضوية ممثلين عن جهات حكومية متعددة، ومن ذلك ممثل عن (وزارة الدفاع - وزارة الداخلية - المخابرات العامة هيئة الرقابة الادارية.. إلخ[5]) وقد ينعكس هذا التشكيل على مدى استقلالية المركز عن السلطة التنفيذية، وفعالية حماية البيانات، بالنظر إلى حجم السلطات الممنوحة للمركز في سياق البيانات الشخصية.

---

[1] انظر المادة (15) من القانون رقم 61 لسنة 1963 بشأن إصدار قانون الهيئات العامة.

[2] انظر المادة (120) فقرة (2) ، لائحة الاتحاد الاوروبي لحماية البيانات العامة.

[3] انظر المادة (120) فقرة (1) لائحة الاتحاد الاوروبي لحماية البيانات العامة : المادة (52) فقرة (4) لائحة الاتحاد الاوروبي لحماية البيانات العامة

[4] انظر المادة 52 من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016 .

[5] انظر المادة 20 من قانون حماية البيانات الشخصية المصري المعنية بتشكيل مجلس إدارة المركز.

الفرع الثاني

الاطار الجزائي لقانون حماية البيانات الشخصية.

اتجه التشريعات المقارنة إلى تنويع أدواتها العقابية لتضمن لنفسها مرونة في مواجهة الاحتمالات المختلفة لانتهاكات البيانات الشخصية[1] ، لذلك نص الفصل الرابع عشر من القانون المصري الخاص بالجرائم والعقوبات على نوعين من العقوبات على اختلاف الجرائم: عقوبات مالية تتمثل في الغرامات متفاوتة المقدار، والعقوبات السالبة للحرية وصورتها الحبس، وجعل المحكمة المختصة بهذا القانون هي المحكمة الاقتصادية .

وباستقراء نصوص قانون حماية البيانات يتضح أن المشرع المصري قد اتخذ من العقوبات المالية وتحديدا عقوبة الغرامة سلاحا أساسيا للتعامل مع تهديدات البيانات الشخصية، فالنصوص العقابية، والتي تبدأ من المادة (35) إلى المادة (48) من القانون، قد جعلت من الغرامات عاملا مشتركا بينها، إذ تم النص على الغرامات كخيار أساسي أو وحيد في كل المواد .

ووفقا للقانون فإن الحد الادنى للغرامة في القانون مائة ألف جنيه والحد الاقصى خمسة ملايين جنيه بحسب الجريمة، والقانون في ذلك يكون قد ساير التشريعات المقارنة وعلى رأسها اللائحة الاوربية لحماية البيانات (GDPR) والتي تعتمد بشكل أساسي على الغرامات . وقد تبنت اللائحة الاوروبية (المادة 83 بند 4)ً تقسيما وحيداً للغرامات، ووفقا لهذا التقسيم يكون الحد الاقصى للغرامة هو عشرة ملايين يورو أو 2 %من الدخل السنوي الاجمالي للجهة في حالات معينة، وترتفع الغرامة في حالات أخرى لتصل إلى 20مليون يورو أو 4 %من الدخل الاجمالي كحد أقصى (م 83 بند 5) .

والملاحظ بالنسبة للقانون المصري فقد آثر المشرع أن يكون اكثر تفصيلا في هذا الصدد، فجعل نطاق العقوبة يتفاوت بحسب كل فعل أو مجموعة أفعال دون أن يجعله نطاقا عاما لجميع الانتهاكات [2].

وفي هذا الصدد نتناول انعكاس التمييز بين البيانات الشخصية العادية والحساسة على المعاملة العقابية، ونطاق الغرامات ومدى فعاليتها في العموم.

أولا : التمييز بين البيانات الشخصية العادية والحساسة من حيث المعاملة العقابية : أشارت الدراسة إلى أن القوانين تعنى كثيرا باضفاء مزيد من الحماية على البيانات الشخصية الحساسة، فهي لم تكتف بوضع قيود أكثر على عمليات المعالجة التي تتضمن بيانات شخصية حساسة فحسب، بل وقامت بمد هذه الحماية لتشمل عقوبات أكثر غلظة على الانتهاكات المتعلقة بها. فبينما أقر القانون المصري عقوبة تتراوح بين 100 ألف ومليون جنيه للانتهاكات الواقعة على البيانات الشخصية العادية، فقد قفز بهذه العقوبة إلى خمسة أضعاف فيما يتعلق بالبيانات

[1] حسام محمد نبيل الشنراقي: حماية البيانات الشخصية عبر الانترنت التحديات والحلول، بحث منشور في المجلة العربية للادارة، ملحق العدد الثاني، المجلد 38 ،2018 ، ص48 .

[2] د. احمد رجب السيد صميدة ، مصدر سابق ، 702 .

الشخصية الحساسة، فنص على نطاق غرامة بين 500 ألف و 5 ماليين جنيه [1]، ذلك ً علما بأن ذلك هو الحد الاقصى للعقوبات المالية المنصوص عليها في القانون كما تمت الاشارةُ سلفا [2].
كذلك، بالنسبة للبيانات الشخصية العادية، قام المشرع المصري بالتمييز بين حالة التعامل غير المشروع على البيانات الشخصية العادية - المذكور سلفا - الذي يتم بغرض الحصول على مقابل مادي أو أدبي، أو لتعريض الشخص للخطر أو الضرر، وحالة التعامل الذي يتم لغير ذلك من الاغراض [3]. ذلك أن القانون قد ضاعف الحدين الادنى والاقصى للغرامة على انتهاك خصوصية البيانات العادية إذا كان ذلك الانتهاك مقابل منفعة مادية أو معنوية، أو كان الانتهاك للاضرار بالشخص المعنى بالبيانات أو تعريضه للخطر، لتصبح الغرامة من 200 ألف جنيه إلى 2 مليون جنيه، أو الحبس لمدة لا تقل عن ستة أشهر. هذا التمييز له أهمية كبرى، لانه يعالج أحد أكبر التهديدات التي تواجه البيانات الشخصية، ألا وهو الاتجار في البيانات، وبالمثل يواجه الاغراض الخبيثة لمعالجة البيانات الشخصية كالتعريض للخطر أو الاضرار .

وان التصدي لذلك السلوك يعد أحد الاهداف التي صيغ القانون من أجلها في المقام الاول؛ فهو إن كان يستهدف حماية البيانات الشخصية في العموم، فهو يبتغي حمايتها من التحديات التي تطرحها التكنولوجيا تحديدا والتي جعلت تداول تلك البيانات والولوج إليها أسهل بكثير، مما يعني أصبحت فرص الاستفادة من تلك البيانات واستغلالها أكبر من ذي قبل، وصارت مادة خام وجاذبة للاتجار فيها والتعامل عليها لاهداف مختلفة [4]. لذا كان من الضروري أن يكون للمشرع موقف أكثر شدة من مسألة المعالجة غير المشروعة للبيانات الشخصية التي تتم بهدف الحصول على مقابل فلا تصبح تلك البيانات سلعة قابلة للتداول. والمجالات التي قد تعتمد على البيانات الشخصية ويستدعي التعامل على هذه البيانات متنوعة للغاية بحيث لا يتسع لعرضها المقام، إلا أنه وعلى سبيل المثال فإن البيانات الشخصية تعد سلعة قيمة جدا في مجال التسويق التجاري بحيث قد تدفع مقابلها مبالغ طائلة[5]. والامر كذلك فيما يتعلق باستخدام البيانات للاغراض السياسية ومحاولة فهم الساحة السياسية والتأثير عليها، ومثال ذلك قضية كامبريدج أناليتيكا الشهيرة التي استخدمت فيها البيانات الشخصية لمستخدمي تطبيق الفيس بوك لتصميم الحملة الانتخابية الرئاسية لاحد المرشحين بحيث تتناسب مع توجهات قاعدة الناخبين [6].

أما وإن كان التمييز بين التعدي على البيانات بحسب الغرض خطوة محمودة إلا أن تحديد الحد الاقصى للغرامة بمبلغ 2 مليون جنيه قد لا يفي بالغرض بعد كل شيء، حتى مع القول بأن

---

[1] انظر نص المادة 41 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .
[2] د. منى الاشقر، د. محمود جبور، مصدر سابق، ص 81.
[3] د. عمرو طه بدوى محمد ، مصدر سابق ، ص69 .
[4] د. رنا أبو المعاطي محمد الدكروري ، مصدر سابق ، ص 232 .
[5] د. سامية عبد الرزاق خلف ، التعدي على حرمة الحياة الخاصة باستخدام التكنولوجية الحديثة ، مجلة الدراسات القانونية ، العدد 25 ، 2010 ، ص115 .
[6] Final Order of the Federal Trade Gommission of the United Stated of America in the Matter of Cambridge Analytica, LLG , a corporation , docket no . 9383, issued at November,25,2019,available,at,{https;//www.ftc.gov/system/files/documents/cases/d09389-comm-final-orderpublic.pdf}

الغرامة ليست الجزاء المالي الوحيد الذي يمكن توقيعه على المعتدي على البيانات، وأنه يمكن تغريمه بتعويض لصالح المتضرر بجوار الغرامة وهو ما سنتناوله في المسؤولية المدنية. ذلك أن تحديد مبلغ التعويض يكون بناء على معيار شخصي بخلاف الغرامة ، أي أنه يتحدد بناء على ما لحق بالشخص المعنى بالبيانات من ضرر أو فاته من كسب جراء تلك المعاملة غير المشروعة. فالغرض من التعويض إذا هو جبر الضرر الذي خلفه الفعل غير المشروع للمضرور. ولكن بالنسبة للغرامة فالغرض منها يمتد لتحقيق الردع، ولذا فيتوقع أن تتجاوز قيمتها ما يمكن تحقيقه من مكسب من وراء الاتجار في البيانات أو على أقل تقدير أن تتساوى مع ذلك المكسب بحيث تسلب انتهاك البيانات كل قيمة له ، ويجد المتعدي المحتمل على البيانات أنه يعرضٍ نفسه لمخاطرة بدون مقابل مجز عندما يحسب تكلفة الفرصة البديلة قبل الاقدام على فعله.

وبالنظر على ما يقتضيه ذلك من الجانب العملي نجد أن شراء بعض قواعد البيانات الشخصية قد يتجاوز سعره الملاين، بل وقد يتجاوز الحد الاقصى لبعض السلع المهمة في الحياة . فكما أشرنا للتو، فإن سوق البيانات الشخصية نشط للغاية وهناك العديد من المجالات والتطبيقات التي تعنى بهذا النوع من البيانات وهي على استعداد لدفع مبالغ ضخمة من اجل الحصول عليها ، هذا التمييز في العقوبة المبني على الغرض من انتهاك البيانات لم يطبق على البيانات الحساسة، فالعقوبة، أو نطاق العقوبة بالادق، واحد بصرف النظر عما إذا كانت تلك المعالجة غير المشروعة تمت بمقابل منفعة أو بغرض تعريض شخص للخطر، أو الضرر أم لا. أي أن أي تعدي على البيانات الشخصية الحساسة يقابله جزاء واحد أيا كانت نية المتعامل في تلك البيانات، ألا وهو الحبس الذي لا يقل عن ستة أشهر أو الغرامة التي تتراوح بين 500 ألف و5 ماليين جنيه.

وبالنظر إلى أن ذلك هو أعلى حد أقصى وحد أدنى لغرامة في القانون، فإن المشرع المصري يكون قد أراد أن يمنح البيانات الحساسة أعلى مستوى من الحماية في كل أصنافها؛ فآثر التعميم بدلا من أن ينص على حد أقل من (500 ألف - 5 مليون جنيه) لحالات الانتهاك .

و يكون ذلك التنويع في المعاملة بين البيانات الشخصية العادية والحساسة مؤديا للغرض منه؛ فهناك حدين للغرامة في البيانات العادية بحسب الغرض من الانتهاك، وهو ما يتناسب مع كونها بطبيعة الحال الاكثر انتشارا والاكثر استخداما وتداولا. وهناك حدٌ واحد للغرامة على انتهاك البيانات الشخصية الحساسة لتحصينها بالكامل وبشكل أكثر صرامة [1].

ومقدار الغرامة ليس هو الضمانة العقابية الوحيدة التي ألحقها القانون بالبيانات الشخصية الحساسة، بل زاد على ذلك بأن وسع النطاق الموضوعي للافعال المجرمة والتي تمثل انتهاكا للبيانات الشخصية الحساسة؛ إذ أنه بالنسبة للبيانات الشخصية العادية قد تم تجريم عمليات "الجمع، والمعالجة، والافشاء، والاتاحة، والتداول" في غير الاحوال المصرح بها قانونا وبغير موافقة الشخص المعني بالبيانات [2]. أما بالنسبة للبيانات الشخصية الحساسة اضيفت إلى تلك الافعال عمليات أخرى تشمل "التخزين، والنقل، والحفظ" [3]، وهذا ما يثير التساؤل؛ فالمفترض في نطاق حماية البيانات أن كافة أنواع البيانات الشخصية تتمتع بالحماية

[1] د. رنا أبو المعاطي محمد الدكروري ، المصدر السابق ، ص 237 .

[2] انظر نص المادة 36 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[3] انظر نص المادة 41 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

ضد كل العمليات التي تشكل تهديد لامنها، ولا اختلاف في ذلك بناء على نوع البيانات إن كانت عادية أو حساسة، والاختلاف يكون فقط في ضمانات الحصول على هذه البيانات والعقوبات الموقعة جزاء لانتهاكها، بحيث يتم كفالة مستوى أعلى من الحماية للبيانات الشخصية الحساسة، لكن التهديدات ينبغي النظر إليها بعين واحدة [1] . لذا حين يعد المشرع بعض العمليات (التخزين، والنقل، والحفظ) محظورة فقط في سياق البيانات الحساسة دون العادية، فإن ذلك يعوزه التبرير، ولا يغني فيه فكرة أنه محاولة لمنح حماية أكبر، لانه كما أوضحنا سلفا فإن مجال زيادة الحماية يكون في العقوبات وشروط جمع البيانات وموافقة الشخص المعنى بالبيانات، وليس طبيعة العمليات الواقعة على البيانات .ومما يعضد ذلك النظر هو أن قانون حماية البيانات الشخصية المصري ، شأنه في ذلك شأن المعايير القياسية العالمية ومنها ال (GDPR)، قد اعترف في المواد (4) و(5) بالحق في النسيان دون تمييز بين البيانات الشخصية العادية والحساسة، وهو ما يعني أن عمليات " التخزين والحفظ والنقل" بطبيعة الحال يجب أن يكونوا مشروعين في كل الاحوال، وهو ما يطرح التساؤل حول الحكمة من وراء اختصاص البيانات الشخصية الحساسة بحماية خاصة في هذه العمليات الثلاث ؟ .

اذ ان هذه البيانات تتمتع بقدر عال من الحساسية كونها تتعلق بمعلومات خاصة جدا بالنسبة للزبون قد لا يريد الإفصاح عنها او تخزينها او معالجتها ، ولذلك شدد المشرع في حمايتها وفرض جزاءات كبيرة على المخالف للحكام المتعلقة بها .

ومن حيث النطاق الشخصي يرى الباحث أن المشرع المصري قد ساوى بين البيانات الشخصية العادية والحساسة بأن جعل من الحائز والمتحكم والمعالج، كلهم مخاطبين بكلا النصين الخاصين بالبيانات الشخصية العادية والحساسة .

وبذلك يكون القانون قد أحاط البيانات الشخصية الحساسة بسياج عقابي شديد، في اعتراف منه بمدى حساسية ذلك النوع من البيانات؛ حيث أن سوء استخدامه والتعدي عليه يسبب أضرارا أكثر جسامة من مجرد التعرف على الشخص أو التوصل إليه، وقد يساء استخدامه بما يضر بالامن القومي والفردي، حيث إن التعرف على التوجهات الدينية والسياسية والبيانات الحيوية للافراد، قد يستخدم في توجيه الافراد، أو استغلالهم، أو الترصد بهم وتقييد حريتهم في التعبير، أو حتى ابتزازهم [2] .

ثانيا : نطاق الغرامات وفعاليتها : تبنى المشرع المصري في قانون حماية البيانات الشخصية المصري نطاقا للغرامات، حده الادنى 100 ألف جنيه والاقصى 5 مليون جنيه، تبعا لاختلاف الجرائم.المنصوص عليها في القانون المذكور، ومن خلال تتبع نهج المشرع لدى وضع الحدين الادنى والاقصى لكل فعل من الافعال، يمكن أن يستنتج ترتيب أولويات المشرع المصري والاعتبارات الاكثر حاجة للحماية في نظره والاقل [3]. فبالنظر في طبيعة العقوبات المالية للقانون يتضح أن القانون قد قسم الغرامات إلى أربع فئات رئيسية : الجرائم فئة المليون جنيه كحد أقصى، وفئة المليونين، وفئة الثلاثة ملايين، والخمسة ملايين وهي الاكبر . فالمخالفات الاكثر خطورة في نظر المشرع كانت ثلاث: أولها الانتهاكات التي تنصب

[1] د. راشد طارق جمعة السيد ، مصدر سابق ، ص 20 .

[2] د. وسيم شفيق الحجار ، مصدر سابق ، ص191 .

[3] د. محمود رجب فتح الله ، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري رقم 175 لسنة 2018 ، دار الجامعة الجديدة ، الإسكندرية ، 2019 ، ص785 .

على البيانات الحساسة التي نص في المادة (41) على العقاب عليها بالحبس ما لا يقل عن 3 أشهر أو الغرامة التي تتراوح بين 500 ألف و5 ملايين جنيه والتي تخاطب كل من الحائز والمتحكم والمعالج ، وتحظر عليهم جمع أو إتاحة أو تداول أو معالجة أو إفشاء أو تخزين أو نقل أو حفظ البيانات الشخصية الحساسة بدون موافقة الشخص المعنى بالبيانات أو في الاحوال المصرح بها قانونا[1].كذلك اعتبر المشرع المصري مخالفة أحكام التراخيص والتصاريح والاعتماد أحد المخالفات التي تستحق الفئة الاعلى من الغرامات أيا كان المخالف وهو ما يشمل بطبيعة الامر الحائز والمتحكم والمعالج، وكذلك من يمارس نشاط تقديم الاستشارات في مجال حماية البيانات .أما الحالة الثالثة فتشمل مخالفة أحكام حركة البيانات العابرة للحدود المذكورة في المواد (14)و (15)و(16) وتلك الحالة ، وإن كان المشرع لم يخاطب بها شخص معين، فنطاقها الشخصي المنطقي يمتد إما للمتحكم أو للمعالج لانهم هم من يملكون تمرير البيانات عبر الحدود .وعلى صعيد آخر، يتم توقيع الفئة الاقل من الغرامات (من 100ألف إلى مليون جنيه) على الحائز والمتحكم والمعالج الذين يتخلفون عن الحصول على موافقة الشخص المعني بالبيانات للقيام بالمعالجة، أو حال قيامهم بها دون الحالات المصرح بها قانونا . ووفقا للمادة (37) تنصب ذات الغرامة على نفس الاشخاص إذا ما أعاقوا الشخص المعنى بالبيانات من ممارسة حقوقه[2] .

ومما تقدم يمكن القول بأن الشريحة الاقل من العقوبات خص بها المشرع الانتهاكات المتعلقة بحقوق الشخص المعني بالبيانات. بينما تقع في المنتصف العقوبات المتعلقة بالتزامات المتحكم والمعالج، والعاملين بالمركز، ومسؤول حماية البيانات، والمخالفات التي تتعلق بأحكام التسويق الالكتروني للبيانات .هذا التدرج في الغرامات والذي يعكس ترتيب الاولويات بالنسبة للمشرع المصري لم يكن هو ذاته الذي تبنته اللائحة العامة لحماية البيانات (GDPR)[3] ، فوفقا للمادة (83)من تلك اللائحة، تم تقسيم الغرامات إلى فئتين فقط: أما الفئة الاولى فتوقع حد أقصى للغرامة يتمثل في الاعلى قيمة بين 10 ملايين يورو أو 2 % من الدخل العالمي الاجمالي للشركة أو للمؤسسة، بينما تشمل الفئة الثانية الاعلى قيمة الغرامة بين 20 مليون يورو أو 4 %من حجم أعمالها، ودون أن يكون لاي منهم حدود دنيا، وهو ما يعطي مرونة أكثر للجهة المختصة بتوقيع العقوبة . وعلى خلاف القانون المصري، فإن الفئة الثانية للغرامات وهي الاعلى تشمل انتهاك حقوق الشخص المعنى بالبيانات، ومبادئ المعالجة وعلى رأسها موافقة الشخص المعنى بالبيانات، أما مخالفات التراخيص فقد تم ادخالها في الفئة الاولى وكذلك التزامات المتحكم والمعالج .بوجه عام، قام المشرع باتباع النهج العالمي في العقاب على انتهاكات البيانات الشخصية بأن تبنى نطاق كبيرا للغرامات، فحتى وإن كانت قيمة الغرامات في القانون المصري تبدو منخفضة مقارنة باللائحة الاوربية، فذلك لا يمنع أنها تعد مرتفعة إذا ما قورنت بمعدل الغرامات في القوانين المصرية الاخرى، وتحديدا القوانين المتعلقة بالتكنولوجيا [4]، على

---

[1] د. رنا أبو المعاطي محمد الدكروري ، المصدر السابق ، ص 257 .

[2] - أشارت هذه المادة لحقوق الشخص المعنى بالبيانات المذكورة في المادة 2 ،ً تحديدا: العلم والاطلاع، والعدول، والتصحيح والتعديل، وتخصيص المعالجة، والعلم بالخرق، والحق في الاعتراض.

[3] د. احمد رجب السيد صميدة ، المصدر السابق ، 709 .

[4] -يلاحظ أن الغرامات التي نص عليها قانون حماية البيانات الشخصية المصري تختلف من حيث طبيعتها عن تلك التي تتضمنها اللائحة الاوروبية، حيث أن الغرامة فيً مصر تعد عقوبة جنائية بينما هي غرامة إدارية وفقا للائحة الاوروبية، وهو ماٍ يترتب عليه اختلاف الاختصاص بتوقيع الغرامة في كل من النظامين. ففي أوروبا

سبيل المثال يقل متوسط الغرامات المنصوص عليها في قانون جرائم تقنية المعلومات عن 500 ألف، والحد الاقصى للغرامات في ذلك القانون هو مليون جنيه - إلا في حالة امتناع مقدم خدمة عن الامتثال لحكم محكمة وأن يترتب عليه الاضرار بالامن القومي أو وفاة أحد الاشخاص فتصبح الغرامة بين 3 ملايين و20 مليون جنيه (م 30 قانون جرائم تقنية المعلومات . بيد أنه متى كان التزام المتحكم أو المعالج أو الحائز يتعلق بعدم الاحتفاظ بالبيانات لمدة أطول من اللازم للوفاء بالغرض المحدد لها [1] ، وكانت العقوبة التي توقع جراء عدم التقيد بذلك هي الغرامة التي تتراوح بين 200 ألف و 2 مليون جنيه ، فإن مقدم الخدمة - سواء أكان متحكم أو معالج أو حائز- يقع عليه التزام قانوني مقابل الاحتفاظ بالبيانات ً لمدة معينة [2]، فوفقا لقانون جرائم تقنية المعلومات يتوجب على مقدم الخدمة أن يحتفظ بالبيانات التي تمكن من التعرف على مستخدم الخدمة (الشخص المعنى بالبيانات) لمدة مائة وثمانين يوما متصلة. وقد قرر ذلك القانون غرامة تتراوح بين 5ملايين و 10 ملايين جنيه في حالة عدم الامتثال، وتضاعف في حالة العود (مادة 2 من قانون جرائم تقنية المعلومات) مما يعني يصبح هناك استثناء على الحق في النسيان والالتزام بعدم الاحتفاظ الواقعين على المتحكمين والمعالجين، وهو استثناء غير تقديري، أي يلتزم به مقدم الخدمة بشكل مطلق أيا كانت طبيعة البيانات المحتَفظ بها، دون الوقوف على إرادته أو إرادة الشخص المعنى بالبيانات، وجزاء عدم الانصياع له يتجاوز حتى الحد الاقصى للغرامة في قانون حماية البيانات الشخصية ككل .وفي إطار تحديد نطاق الغرامات يلاحظ أن القانون قد أغفل ذكر معايير لتحديد قيمة الغرامة، فترك الامر لسطلة القاضي والتفريد القضائي للعقوبة دون إعطاءه معايير يسترشد بها، وهو مسلك يخالف ما ذهبت إليه اللائحة الاوربية (GDPR) فى المادة 83 منها، إذ تحدد مجموعة عوامل تساعد على تقدير الغرامة بحسب طبيعة وجسامة الانتهاك الواقع، وما إذا كان عمديا، ومحاولات المتحكم أو المعالج لتدارك الخرق وغيرها [3]. وعلى ذلك يكون قد ترك أمر التدرج بالعقوبة للقاضي ولما تأتي به اللائحة التنفيذية ايضا[4] .

تختص مراكز حماية البيانات بتقدير الغرامة وتوقيعها وتخفيفها، بينما ينصرف ً ذلك الاختصاص للمحكمة وحدها في مصر. ويعني ذلك أيضا خضوع الغرامات في مصر باعتبارها غرامات جنائية لكافة قواعد العقوبات الجنائية؛ فهي تخضع لمبدأ الشرعية، ولمبدأ شخصية العقوبة، وتتعدد بتعدد الفاعلين، وهو ما يعني إمكانية خضوع أكثر من متحكم أو حائز للغرامة كل على حدة عن نفس الفعل ، انظر الدكتورة رنا أبو المعاطي محمد الدكروري ، ص 302 .

[1] انظر نص المادة 3 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[2] د. بهاء المري ، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الاثبات ، ط1، العربية للنشر والتوزيع ، مصر ، القاهرة ، 2018 ، 182 .

[3] كذلك ذهبت بعض الدول إلى أبعد من ذلك، فتبنت الهيأة المعنية بالتنسيق بين السلطات الرقابية على حماية البيانات في ألمانيا (DSK)آلية لحسابة قيمة الغرامات المفترض توقيعها على المخالفين.

https//:iapp.org/news/a/german-dpas-push-model-for-higher-gdpr-fines/-

[4] Paul Lambert , DATA Protection, DATA Loss and Penalties , (2012)4 IBLQ 22,P26 ; recital 13 , GDPR .

المطلب الثاني

اشكالات الضمانات القانونية لحماية البيانات الشخصية

تعكف التشريعات الدولية والداخلية على البحث في كل مرة عن الحلول المجدية لضمان حقوق الأشخاص ووقف التعدي عليها ، وتقليل حدة انتهاك الخصوصية وحماية البيانات الشخصية خصوصا بعد تنامي خطر انتشار الجرائم المعلوماتية والتعدية على حياة الزبائن الخاصة ، ان لم نقل القضاء على هذه الظاهرة بشكل تام ، على الرغم من ان الكثير من المحاولات تعترضها العديد من الإشكالات الموضوعية والاجرائية ، مما يؤكد خصوصية ضمان حماية البيانات الشخصية ، مقارنة بغيرها من المحال التقليدية موضوع الحماية القانونية .

وسنحاول من خلال هذا المطلب التطرق لمختلف تلك الإشكالات في ضوء ما هو مستقر في التشريعات محل المقارنة ، لكن تقسيمنا المنهجي للاشكالات او الصعوبات المرتبطة بضمانات حماية البيانات الشخصية لا ينبني على أساس ما هو موضوعي واخر اجرائي ، بل سيتم تناوله من خلال التركيز على الصعوبات المرتبطة بازدواج نصوص التجريم ، وكذلك الصعوبات المتعلقة بالقانون الواجب التطبيق من جهة ثانية ، وأخيرا الصعوبات المرتبطة بخصوصية الاثبات والتحقيق في هذا النوع من الاعتداء وكالاتي :

الفرع الأول

ازدواج نصوص التجريم

باستقراء النصوص العقابية في قانون حماية البيانات يتبدى بعض الالتباس بخصوص بعض الافعال المجرمة، فقد تناول المشرع مثلا فعل "جمع" البيانات غير المشروع الصادر عن المتحكم بالتجريم في موضعين مختلفين دون اختلاف ظاهر في شروط التطبيق مع اختلاف العقوبة [1]. فالمادة (36) من القانون تنص على أن "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تتجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع... بيانات شخصية... في غير الاحوال المصرح بها ً قانونا أو بدون موافقة الشخص المعني بالبيانات". وفي المادة (38) يعود المشرع فيخاطب المتحكم أو المعالج مرة أخرى بالعقاب "بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تتجاوز ثلاثة ملايين جنيه" إذا لم يلتزم بواجباته المنصوص عليها في المادة(4) وتنص الاخيرة بدورها على أن "يلتزم المتحكم بالحصول على البيانات الشخصية أو تلقيها من الحائز أو المتحكم أو من الجهات المختصة بتزويده بها بحسب الاحوال بعد موافقة الشخص المعنى بالبيانات أو في الاحوال المصرح بها قانونا. والالتزام هنا يدخل كذلك تحت مفهوم جمع البيانات أيضا، ليصبح هناك وحدة في الموضوع والشخص واختلاف في العقوبة وهو ما يمثل ازدواج في نصوص التجريم والعقوبة على السواء[2].

وقد تكرر الامر ذاته بالنسبة لاتاحة البيانات وإفشائها، فذات المادتين (36)و(38) يوقعان نفس العقوبات سالفة الذكر على فعل إفشاء البيانات الشخصية، بيد أن المادة (36)تشير إليه بوصف إفشاء البيانات، بينما تشير المواد (4)و(5)المحال إليهما من المادة (38)بوصف "القيام

---

[1] د ، بهاء المري ، مصدر سابق ، ص 203 .

[2] د. احمد رجب السيد صميده ، مصدر سابق ، ص310 .

بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات"، وهو ما لا يتصور اختلافه في المضمون عن الافشاء، وبالتالي نكون مرة أخرى أمام وحدة موضوع (الافشاء) ووحدة أشخاص (المتحكم والمعالج)، مع اختلاف العقوبة[1] .

ومن المواضع التي قد تثير اللبس أيضا العقوبات على مخالفة التراخيص والتصاريح، إذ توقع المادة (38) جزاءا عاما على مخالفة المتحكم لمجموع التزاماته المذكورة في المادة (4) ومخالفة المعالج لمجموع التزاماته المذكورة في المادة (5)، ومن بين هذه الالتزامات الالتزام "بالحصول" على التراخيص والتصاريح، بينما توقع المادة (45)عقوبة الغرامة التي تتراوح بين 500 ألف جنيه و 5 مليون جنيه في حالة "مخالفة أحكام التراخيص والتصاريح". إلا أن المادة الاخيرة لا تخص المتحكم والمعالج وإنما تخاطب كل من يخالف أحكام التراخيص والتصاريح. وذلك النطاق الشخصي وإن كان أوسع فإنه من غير المتصور أن يقتصر على المتحكم والمعالج باعتبار أنهما المخاطبين الرئيسيين بالتزامات التراخيص والتصاريح مثلما اشارت لذلك محكمة النقض الفرنسية [2] .

اما بخصوص القضاء باعتباره الضامن والحارس الأساسي للحريات والحقوق ، والذي يقوم بمهمة المراقبة على اعمال المؤسسات التنفيذية ومن ضمنها التي تعنى بحماية الخصوصية والبيانات الشخصية ، فان ابرز مظاهر محدودية دوره المهم في تطبيق قواعد القوانين وتطبيق غاياتها وأهدافها ، تتمثل في ضعف الخبرة والتكوين في مجال التكنولوجيا والجرائم المعلوماتية بشكل عام ، وجرائم معالجة البيانات الشخصية بشكل خاص ولا يساير على غرار القوانين وجهات البحث والتحري التطور التكنولوجي في مجال المعلوماتية ، مما يثير نوعا من الارباك في ضمان تطبيق فعال يتماشى مع غايات المشرع في حماية البيانات الشخصية للزبائن .

وفي ختام هذا الفرع نشير الى ان العراق دخل عالم الثورة الرقمية من حيث التحول الاقتصادي وكذا الاجتماعي ، والتي عززها المشرع بعدة تشريعات تواكب التطورات المعلوماتية و التكنولوجية في العديد من المجالات خاصة التحويلات المالية والتجارة الالكترونية ، ومن اجل مسايرة القوانين الدولية والإقليمية التي تعنى بهذا الشأن كاللائحة الاوربية (GDPR) ، على رأسها دستور العراق الدائم لسنة 2005 الذي نص على حماية الحياة الخاصة ، ثم قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (78) لسنة 2012 ،الى جانب قانون المصارف رقم 94 لسنة 2004 ، وقانون البنك المركزي رقم 56 لسنة 2004 ، وهناك مشروع قانون مكافحة الجرائم الالكترونية لسنة 2019 ، والذي لم يرى النور الى الان ، الا انه لازال دون مستوى الطموح وبحاجة لسن تشريعات تنظم حماية البيانات الشخصية وتبين طريقة التعامل بها ، مثلما موجود في بعض القوانين بالمنطقة العربية .

وقد جاء المشرع العراقي بمجموعة من الضمانات المؤسساتية والقانونية لتطبيق قواعد حماية البيانات الشخصية وان كانت ليست بهذا العنوان ، والتي تتلائم في بعض مضامينها مع التوجهات الاوربية ، فالقانون العراقي لم يجز المساس بخصوصية البيانات الشخصية الا في حالات ضرورية مثالها السرية المصرفية اذ اوجب المشرع العراقي على المصارف وفقا للمادتين (49 -50) من قانون المصارف النافذ بعدم افشاء أي بيانات تتعلق بعملاء المصرف او حساباتهم او ودائعهم او الامانات او الخزائن الخاصة بهم او أي من معاملاتهم او كشفها او تمكين طرف ثالث من الاطلاع على هذه المعلومات والبيانات من غير

[1] د. عثمان بكر عثمان ، مصدر سابق ، ص22 .

[2] Cass .Crim , 14 Mars ,2006 , disponible sur www.Legi France .gouv-Fr .

الحالات المسموح بها بمقتضى احكام هذا القانون ، لنجد ان القانون نفسه وبالمادتين المذكورتين يجيز افشاء تلك البيانات في حالات عدة منها الموافقة الخطية من الزبون المعني نفسه . كذلك اشارت المادة الخامسة من قانون البريد العراقي على جواز الاطلاع على المراسلات البريدية لضرورات العدالة والامن في الأحوال التي يجيز فيها القانون ذلك . وعليه فان الهدف من هذه التشريعات وغيرها هو تحقيق الغاية المرجوة منها وهي حماية حريات و حقوق الزبائن وهي :

1- الحماية الجنائية : وتبقى هي اهم مظاهر الحماية القانونية في أي مجال كون العقوبة الجزائية تهدف الى تحقيق الردع الخاص والعام ، وهي تعد في الوقت الحاضر اقصى درجات الحماية التشريعية للمصالح الفردية والجماعية والقيم المجتمعية [1]، واعتى ما تملكه الدول في ترسانتها خاصة في ظل محدودية الجزاءات الإدارية والمدنية في مواكبة الخطورة الاجرامية لبعض الأفعال المستحدثة كما هو الحال في العراق على سبيل المثال .

2- اما الجهات المؤسساتية فلا يوجد في العراق جهة محددة تتولى هذه المهمة ، ولكن يبقى الأسلوب التقليدي في العمل القضائي وهو انتداب الخبراء سواء كان من الجهات الأمنية كما في جهاز الامن الوطني او خلية الصقور ، او اذا كان الامر متعلق بموضوع إذاعي او اتصالات فيتم الاستعانة بهيأة الاعلام والاتصالات، وتبقى هذه الجهات تحت رقابة واشراف القضاء وذلك لضمان ثقة ومصداقية اكبر لهذه المؤسسات امام الافراد .

ورغم كل المحاولات القانونية الا اننا في العراق لازلنا لم نصل الى ما وصلت اليه اغلب الدول بخصوص حماية البيانات الشخصية ، وأيضا مازال المشرع للأسف ينظر الى حق حماية البيانات الشخصية او الحق في الخصوصية من الزاوية القانونية فحسب ، و ايكال امره الى محاكم الجزاء ومحاولة تطبيق العقاب على من ينتهك هذا الحق .

وذلك راجع الى غياب الادراك بأهمية هذا الحق ، وعدم معرفة خطورة المعالجة غير المشروعة للبيانات الشخصية وطرق استغلالها من طرف المجتمع العراقي ، وضعف التوعية اللازمة في هذا المجال ، خاصة ان اول وسيلة لمكافحة مخاطر التقنية المعلوماتية هي الحماية الذاتية [2].

لذلك يتوجب العمل على تشريع القوانين من سلطة تشريعية وتنفيذية ونقابية ان يغيروا نظرتهم القانونية لهذا الحق وغيره من الحقوق الرقمية وينظروا اليه من زاوية حقوق الانسان ، ما دامت الغاية التي اوجدت الحق في حماية البيانات الشخصية هي حماية حق اصلي تقليدي دستوري وعالمي الا وهو الحق في حماية الحياة الخاص ، وخير من نظم هذا الحق بهذا المعنى هي اللائحة الاوربية لحماية البيانات الشخصية (GDPR).

الفرع الثاني

اشكاليات القانون الواجب التطبيق وضعف التنسيق الدولي

تتطلب الحماية القانوني لحماية البيانات الشخصية وجود منظومة تشريعية متكاملة تضمن عدم التعدي عليها ، ولكن هذا الامر يصطدم بمعوقات حقيقية وهي كالاتي :

[1] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات للشخصية ، مصدر سابق ، ص 267 .

[2] د. سوز حميد مجيد ، مصدر سابق ، ص168 .

أولا : الصعوبات المتعلقة بالقانون الواجب التطبيق : من المعلوم ان البيانات الشخصية وحمايتها تتميز بخاصية عالمية ، اذ يشكل الاعتداء عليها عملا عابرا للحدود ، الامر الذي يثير اشكالا قانونيا يتعلق بالقانون الواجب التطبيق على الاعتداء الواقع في البيئة الرقمية ، وما اذا كان القاضي يحتكم الى قانون الدولة التي وقع التعدي في اقليمها ام قانون الدول او الدولة التي حصل الضرر على اقليمها [1].

لذا تقف صفة العالمية التي يصطبغ بها فعل التعدي على البيانات الشخصية حاجزا امام إمكانية متابعة الفاعل [2] ، على اعتبار انه يؤدي الى صعوبة تحديد القانون الواجب التطبيق على هذا النوع من المسؤولية ، ومما يعني عجز قواعد الاسناد التقليدية عن إيجاد حلول للمسألة حتى وان طبقت ، طالما ان التنازع يحصل بين اكثر من تشريعين لمواجهة الاعتداء نفسه [3] .

ومن ثم فمن حيث المبدأ ممكن ان يبقى الاعتداء خارج عن سيطرة او رقابة أي جهة بحيث لايمكن خضوعه لاختصاص تشريع معين ، مما يثير إشكالية تحديد القانون الواجب التطبيق على هذه الواقعة ، اخذين بنظر الاعتبار اجماع الدول تقريبا على إعطاء قانونها الوطني الاختصاص اذا كان الفعل واقعا في اقليمها وكانت نتيجتها فيه وتم رفع الدعوى امام محاكمها ، او مست بالمصالح الأساسية للدول [4] .

لكن هذا الامر يتلاشى امام اختلاف المفاهيم المتعلقة بالبيئة الرقمية وحماية البيانات الشخصية بين الدول ، ذلك ان اغلب الأنظمة في العالم تذهب الى ان الاعتداء على البيانات الشخصية أفعال معاقب عليها ، لكنها تختلف من حيث نطاق تطبيق هذه الحماية ، يفهم من ذلك ان افعالا معينة يمكن ان تبقى خارج عن دائرة الاعتداء اذا لم يوجد نص يؤكد على شمولها ، فرغم أهمية البيانات الشخصية وتزايد مخاطر الاعتداء عليها ، ومساسها بالمصلحة العامة في بعض الأحيان الا ان بعض الدول لم تدرج بعض الأفعال التي تمثل انتهاك لها في دائرة الاعتداء على هذه البيانات ، او قد تكون البيانات ذاتها غير محمية بموجب قوانينها [5]

ومهما يكن من امر فقد ذهب البعض الى اقتراح حلولا عاجلة لمواجهة مشكلة تنازع الاختصاص القضائي في حالة الاعتداء على البيانات الشخصية ، ومن جملة تلك الحلول ضرورة تدخل التنظيم القانوني الدولي في موضوع تحديد الاختصاص دون ترك الامر للتنظيم القانوني الداخلي[6] ، وهو ما اخذ به المشرع الأوربي في اللائحة العامة لحماية البيانات الشخصية (GDPR) [7]

وأيضا ممكن اللجوء الى فكرة الاختصاص الأصلي ، والاختصاص الاحتياطي او الثانوي الذي يلجأ اليه في حالة تعذر الاخذ بقانون الاختصاص الأصلي ووفقا لقواعد يتم الاتفاق عليها في ضوء الاتفاقية المقترحة بهذا الخصوص .

---

[1] See European Crime Prevention Network , Cybercrime ; A theoretical overview of the growing digital threat , EUCPN Secretariat , February 2016 , Brussels , p.11, available at ; eucpn.0rg/sites/default/files/ theoretical – paper-cybercrime-pdf, data of access ; 15 January 2021.

[2] د. صفاء حسن نصيف ، التحديات الإجرائية المتصلة بالجرائم المعلوماتية ، بحث منشور في مجلة العلوم القانونية والسياسية ، تصدر عن جامعة بغداد ، المجلد الخامس ، العدد الثاني ، 2016 ، ص274 .

[3] د. ميسون خلف حمد الحمداني ، مشروعية الأدلة الالكترونية في الاثبات ، بحث منشور في مجلة كلية الحقوق جامعة النهرين ، العدد 2 ، المجلد 18 ، 2016 ، ص226 .

[4] د. صفاء حسن نصيف ، مصدر سابق ، ص 277 .

[5] د. هيثم السيد احمد عيسى ، مصدر سابق ، ص 17 .

[6] د. رضوان اسخيطة ، مصدر سابق ، ص 16 .

[7] انظر نص المادة (3) من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016 .

وفي جميع الأحوال تعتبر مسألة تنازع القوانين وتنازع الاختصاص القضائي من ابرز المعوقات التي تحول دون ضمان حماية البيانات الشخصية ، سيما في ظل عجز قواعد الاختصاص التقليدية عن تحقيق هذا الهدف ، ولا غرابة في ذلك طالما ان تلك القواعد وضعت أصلا لمعالجة حالات التنازع التي تحصل بخصوص أفعال محددة واقعيا وليس افتراضيا ، وهو الامر الذي دفع بالقضاء الى طرح معايير اختصاص بديلة تتلائم مع الطبيعة الخاصة لهذه البيئة الرقمية ، وليس ادل على ذلك ما اقره القضاء الفرنسي عندما بين ان الاختصاص في انتهاكات الصحافة الالكترونية يؤول الى محل تمركز الموقع الذي نشرت الاقوال او المعلومات بواسطته ، وعلاوة على ذلك تختص الجهة القضائية التي يقع في دائرتها المكان الذي ارتكب فيه الخطأ المرتبط بالخصوصية او بحقوق الملكية الفكرية [1] .

ان الحل الأنسب حسب رأي الباحث لتجاوز عقبة تنازع الاختصاص القضائي يتمثل في التسليم التدريجي بتطبيق مبدأ عالمية النصوص التي تحمي هذه البيانات ، وهو امر يقتضي التقاء إرادة الدول حول اطار اتفاقي مشترك يحدد القواعد الموضوعية التي تحمي البيانات الشخصية ، ويرسم في الوقت ذاته الضوابط الإجرائية المتبعة في ملاحقة منتهكها واتخاذ الإجراءات القانونية بحقه .

ثانيا : ضعف التنسيق والتعاون الدولي لحماية البيانات الشخصية : على الرغم من الأهمية التي تكتسبها البيانات الشخصية في الوقت الحاضر ، الا ان التنسيق والتعاون الدوليين بشأنها لم يبلغ درجة الاهتمام الذي تشهده بعض المواضيع الدولية على غرار الابتزاز الالكتروني ، والإرهاب الالكتروني ، لذا يكون من الأهمية بمكان توسيع نطاق هذا التنسيق والتعاون الى جميع مجالات البيئة الرقمية كالمساس بالمصلحة العامة والأشخاص والأموال ، بما فيها حماية بيانات الأشخاص ، من خلال ربط اتفاقيات تعاون بين الدول ، بما يتيح إمكانية تقديم طلب الى سلطات الدولة المعنية من اجل تزويدهم بالمعلومات والأدلة في كل ما يحقق الحماية المرجوة [2].

فاذا كان الاعتداء على البيانات الشخصية يمر عبر شبكات ومواقع الكترونية وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة فانه يمثل اعتداء على مواطني تلك الدولة ، فان ذلك يبرر أهمية امتهان قواعد الاختصاص والقانون الواجب التطبيق ، فيما اذا كانت النظريات والقواعد القائمة في هذا المجال تطال هذا النوع من المسؤولية ام يتعين افراد قواعد خاصة بها في ضوء خصوصيتها ، وما تثيره من إشكاليات في مجال الاختصاص القضائي ، مع ملاحظة ان هذا الاشكال يتفاقم اكثر في ظل امتداد الملاحقة والتحري والضبط والتفتيش خارج الحدود [3]، الامر الذي يتطلب وجود تعاون دولي يكفل حماية البيانات الشخصية للافراد ومنع التعدي عليها من جهة ، ولا ينتهك سيادة الدولة على اقليمها من جهة ثانية .

والواقع ان خاصية العالمية التي تميز البيانات الشخصية قد دفعت اهل القانون الى الدعوة لمواجهة الاعتداء عليها من خلال وضع قواعد اتفاقية تعبر عن تصور دولي موحد من شانه تدارك الثغرات والنقائص التي تعتري منظومة القوانين الداخلية للدول وذلك بهدف الحد من هذا النوع من التعدي[4] .

---

[1] د. محمود محمد لطفي محمود صالح ، أطروحة دكتوراه مقدمة الى كلية الحقوق جامعة طنطا ، 2009 ، ص 319 .

[2] د. احمد رجب سيد صميدة ، مصدر سابق ، ص261 .

[3] د. التريش سايبر ، جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات ، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي ، ترجمة سامي الشوي ، دار النهضة العربية ، القاهرة ، مصر ، 2003 ، ص 58 .

[4] د. منى الأشقر جبور ، د. محمود الجبور ، البيانات الشخصية والقوانين العربية ، الهم الأمني وحقوق الافراد ، المركز العربي للبحوث القانونية والقضائية ، ط1، بيروت ، 2018 ، ص 157.

وفي هذا الاطار تظافرت الجهود من اجل وضع اطار قانوني موحد يحقق حماية حقيقية للبيانات ، ويفرض طريقة معينة لمتابعة من يعتدي عليها ، ويضع عقوبات صارمة على من ينتهكها [1] ، وأيضا ابرام العديد من الاتفاقيات الثنائية والدولية تتعلق بهذه المسألة سواء على المستويين الإقليمي والدولي كما في الاتفاقية الاوربية الامريكية [2] .

فمن المعلوم ان موضوع البيانات الشخصية وحمايتها ظهرت في الدول المتقدمة ، ولا غرابة في ذلك على اعتبار ان تلك الدول كانت سباقة الى استخدام البيئة الرقمية في تعاملاتها العادية والتجارية والمالية وغيرها ، لذلك اول من وضع قوانين لتنظيم التعامل في هذه البيانات هي تلك الدول ، ولايوجد ما يمنع من الاستفادة من تجربتها في ذلك ، وهو ماندعو اليه المشرع العراقي في ان يحذو حذو اغلب التشريعات في المنطقة التي عملت على سن قوانين تتماشى مع ماهو موجود في الاتحاد الأوربي على سبيل المثال

الفرع الثالث

الإشكالات المرتبطة بخصوصية الاثبات

من المسلم به اليوم ان قواعد المسؤولية التي طبقت لفترات طويلة لم تعد لها القدرة على مواجهة التحديات التي احدثتها البيئة الرقمية ، على اعتبار ان المسؤولية هنا ترتبط بفضاء افتراضي غير واقعي ، وتثير هنا اشكالا خاصا يتعلق بمسألة اثباتها ، فلا يزال هذا الموضوع مجالا خصبا للنقاش والتحليل من لدن رجال القضاء والقانون على حد سواء [3] ، وقد برزت أهمية موضوع دليل الاثبات الالكتروني لفعل التعدي على البيانات الشخصية بفعل قصور وسائل الاثبات الإجرائية المعمول بها في دائرة المسؤولية التقليدية التي تتم في البيئة المادية ، عن اثبات التعدي في البيئة الافتراضية [4] .

من المفيد التنويه في هذا الاطار الى ان مواجهة إشكالية اثبات واقعة التعدي على البيانات الشخصية اصبح يتطلب تظافر جهود القانونيين وأجهزة البحث والتحري على المستويين الوطني والدولي ، فاذا كان لا يتعذر في الكثير من الأحيان الوصول الى الدليل المادي بشأن المسؤولية التقليدية فانه من الصعوبة بمكان اثباته فيما يخص انتهاك البيانات الشخصية ، سيما في ظل التطورات التكنولوجية التي يشهدها عالمنا المعاصر ، والتي ساعدت على انتشار ظاهرة التعدي على البيانات الشخصية دون ترك أي دليل مادي يمكن أجهزة التحري من متابعة مرتكبها باستخدام الوسائل التقليدية [5] ، ولا غرابة في ذلك طالما ان من يقوم بفعل التعدي بالعادة يكون محترف ويستطيع الاستفادة من الأساليب والتقنيات التكنولوجية الحديثة للقيام بانتهاك البيانات في مختلف انحاء العالم عبر شبكة الانترنت ، فضلا عن استخدامه ذكاءه وامكانياته العلمية والعملية التي تمكنه من محو الاثار التي يمكن التعرف عليه من خلالها [6] .

---

[1] كما هو الحال في بعض التشريعات العربية التي حذت حذو اللائحة الاوربية العامة لحماية البيانات الشخصية (GDPR)، كالقانون المصري رقم 151 لسنة 2020 ، الاماراتي رقم 45 لسنة 2021 ، وغيرها من القوانين .

[2] The EU-US Data Privacy Framework 2023 .

[3] د. ميسون خلف حمد الحمداني ، مصدر سابق ، ص 209 .

[4] د. طالب جواد عباس ، د. عبد الجبار ضاحي عواد ، الدليل الرقمي واثره في الاثبات ، زين الحقوقية ، بيروت ، 2016 . ص62

[5] د. محمود وهيب ، ظاهرة العولمة وانعكاساتها الأمنية ، بحث منشور في المجلة العربية لعلوم الشرطة ، مطابع الشرطة ، القاهرة ، العدد 164 ، 1999، ص70 .

[6] د. طالب جواد عباس ، د. عبد الجبار ضاحي عواد . مصدر سابق ، ص87 .

ومهما يكن من امر يبقى الدليل الرقمي هو المعول عليه في اثبات تحقق المسؤولية من حيث الزمان والمكان ، لهذا يرى الباحث ضرورة ضبط مدلوله والصعوبات المرتبطة به ، فضلا عن خطورة الاطلاع على البيانات وواجبات الجهات المختصة في المحافظة عليها ، فضلا عن قيمته في الاثبات.

أولا : مدلول الدليل الرقمي والصعوبات المقترنة به : تنوعت وتعددت التعاريف التي قيلت بشأن الدليل الرقمي ، وتباينت بين التوسع في مفهومه والتضييق فيه ، فقد عرفته المنظمة العالمية لدليل الكمبيوتر(IOCE) في عام 2001 بانه (المعلومات ذات القيمة المحتملة والمخزنة او المنقولة في صورة رقمية)[1] ، كما عرفه البعض الاخر على انه(الدليل المأخوذ من أجهزة الحاسب الالي ويكون في شكل مجالات او نبضات مغناطيسية او كهربائية ، بحيث يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ، ويتم تقديمها في شكل دليل يمكن التمسك به امام القضاء) [2] .

يتبين لنا من خلال التعاريف السابقة ان الدليل الرقمي يختلف كثيرا عن نظيره المادي فهو لا يرتبط بالضرورة بمحل المسؤولية بل يستخلص من الوسيلة التي يشتغل بها النظام المعلوماتي ، فهو يوجد حتى قبل القيام بالفعل الذي أدى الى التعدي على البيانات الشخصية ، ولكن هذا لا يفسر سهولة الحصول عليه ، او الاحتجاج به في أي وقت ، ذلك ان ما سبق ينقلب كعائق حقيقي امام الجهات المختصة في الاثبات .

هذا ما يكشف عن وجود صعوبات حقيقية تتعلق بالدليل الرقمي في حد ذاته ، وتتالف من البنية التي يستمد منها الدليل الرقمي وجوده ، والتي تقوم على أساس المعلومات التي تتحرك وتنساب عبر الحواسيب الالية والشبكات في شكل نبضات الكترونية غير مرئية مما يكسب الدليل الرقمي ميزة التخفي ، وغالبا تكون هذه المعلومات مشفرة مما يصعب مسألة الوصول اليها خاصة اذا كانت معلومات خاصة او خطيرة ، وعلى الرغم من اعتماد بعض المؤسسات والشركات ذات الأنظمة المعلوماتية في حماية هذه الأنظمة عن طريق تشفير بيانات زبائنها الشخصية الا بعض الأشخاص لديهم القدرة على اختراق هذه الأنظمة ، وبالتالي تصبح حمايتها غير ذات جدوى سيما اذا كان من العاملين داخل هذه الشركة او المؤسسة [3] .

وان كنا لا ننكر من جهة أخرى ما يسجل للدليل الرقمي من قابليته للنسخ حيث ان من شأن ذلك التقليل او بالأحرى اعدام مخاطر اتلاف الدليل الأصلي ، حيث تتطابق طريقة النسخ مع طريقة الانشاء ، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من التلف عن طريق نسخ طبق الأصل من الدليل [4] .

وإزاء البحث عن الدليل الرقمي يستعين المختصون بمجموعة من الأدوات المادية ، وبرامج التقاط الدليل الالكتروني ومن اشهرها على الاطلاق برامج التتبع ونظام كشف الاختراق [5] .

---

[1] د. د.منى عبد العالي موسى ، مصطفى كريم هادي ، وسائل اثبات جريمة الازعاج بواسطة الوسائل السلكية واللاسلكية ، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية تصدر عن جامعة بابل ، المجلد 26، العدد 9، 2018، ص 484 .

[2] د. طالب جواد عباس ، عبد الجبار ضاحي عواد ، مصدر سابق ، ص 75 .

[3] د. صفاء حسن نصيف ، مصدر سابق ، ص 261 .

[4] د. محمد بن فردية ، الدليل الجنائي الرقمي وحجيته امام القضاء الجنائي ، بحث منشور في المجلة الاكاديمية للبحث القانوني ، تصدر عن كلية الحقوق والعلوم السياسية جامعة بجاية ، السنة الخامسة ، المجلد 9 ، العدد 1 ، 2014 ، ص 283.

[5] يتمثل دور برامج التتبع في التعرف على محاولات الاختراق وتقديم بيان شامل عنها الى المستخدم الذي يتم اختراق جهازه او بيانات شركة معينة ومثاله برنامج (Hack tracer) وهو مصمم للعمل في الأجهزة المكتبية ، وعندما يتم رصد محاولة للاختراق يسارع باغلاق منافذ الدخول امام المخترق ثم يبدأ بعملية مطاردة تستهدف اقتفاء اثر مرتكب عملية الاختراق حتى يصل الى جهاز الذي حدثت منه العملية ، اما بالنسبة لبرنامج كشف الاختراق والذي يرمز له ب IDS فيقوم على أساس مراقبة بعض العمليات التي تتم على مستوى الشبكة او الحاسب ، مع تحليلها بحثا عن وجود أي إشارة تدل على

ثانيا : الجهات التي تتولى البحث عن الدليل : تستهدف عملية التفتيش المعلوماتي البحث في نطاق منظومة معلوماتية او جزء منها وكذا البيانات المخزنة فيها ، ومنظومة تخزين المعلومات ، حيث يمكن القيام بذلك في مكان القيام بفعل التعدي او بعيد عن ذلك .

حيث ينصب التفتيش في مثل هذا الموضوع على مستودع السر الذي يحتفظ فيه الشخص بالاشياء المعنوية او المادية التي تتضمن نشاطاته المنجزة ويشمل كل ماله علاقة بانتهاك البيانات الشخصية محل الاعتداء من برامج والات وكذا أجهزة الحاسوب او الهواتف النقالة وغيرها من الأجهزة الالكترونية التي استعان صاحب الفعل الضار مثل شرائح الهواتف وبطاقات الذاكرة والات التصوير الرقمي .... .

وبالنسبة لهذه الأدلة المبحوث عنها والمخزونة في منظومة معلومات أخرى يمكن القيام بعملية التفتيش بسرعة دون حاجة لاستصدار اذن قضائي من اجل مباشرة العملية [1]، ولعل السبب الذي يكمن وراء هذا الاجراء هو الخوف من اندثار وتلاشي الدليل في حالة إطالة الإجراءات وانتظار الحصول على اذن قضائي لمباشرة عملية تفتيش المنظومة حيث قد يعمد الفاعل الى القيام بعملية اتلاف البيانات والمعطيات التي بحوزته بمجرد وصول الى علمه انه محل متابعة من طرف الجهات المعنية .

كما انه من حق السلطات المختصة بإجراء عملية التفتيش اللجوء او تسخير كل شخص له دراية بعمل المنظمة المعلوماتية محل البحث او بالتدابير المتخذة لحماية البيانات الشخصية بقصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها [2].

اما في حالة كون المعطيات المراد تفتيشها واقعة خارج نطاق إقليم الدولة ، فيمكن الحصول عليها عن طريق التعاون الدولي من خلال طلب المساعدة من السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ، فالتطور التكنولوجي الحاصل في مجال المعلوماتية سهل نوعا ما من اختراق المواقع الالكترونية وسرقة البيانات الشخصية دون ان تكون الحدود الجغرافية عائقا امام الفاعل ، لذلك اصبح من الضروري البحث في مدى مشروعية القيام بالتفتيش ومحاولة الحصول على الدليل الرقمي في نطاق دولة أخرى [3].

ان الحصول على مثل هذه المعلومات دون طلب المساعدة من الجهات الرسمية للبلد الأجنبي يعد بمثابة انتهاك لسيادة ذلك البلد وخرقا للقوانين الوطنية والاتفاقيات الدولية المتعلقة بإمكانية التعاون الدولي في مجال الجرائم المعلوماتية بشكل عام و حماية البيانات الشخصية للافراد بشكل خاص .

ولكن على الرغم الاتفاقيات الدولية الموقعة في هذا الشأن والمشار اليها آنفا والقاضية بإمكانية التعاون في مجال التفتيش المعلوماتي ، الا ان الواقع يكشف ان هناك بعض الدول غير مستعدة لمباشرة هذه الالية كونها تعتبر مثل هذه القضايا بمثابة مساس بالامن الداخلي القومي لها مثلا (أمريكا) خاصة اذا كانت

وجود تهديد ، حيث انه يسجل الاحداث فور وقوعها ، ويقارن نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية وفي حالة اكتشافه لاحدى هذه الصفات يقوم بانذار مدير النظام ويسجل البيانات الخاصة بذلك الاعتداء . انظر في ذلك الدكتور محمد بن فردية ، مصدر سابق ، ص285.

[1] د. شوقي يعيش تمام ، الجريمة المعلوماتية ، مطبعة الرمال ، الجزائر ، 2019 ، ص50 .

[2] د. عبد الرحمن خليفة الرواس ، مصدر سابق ، ص138 .

[3] د.منى عبد العالي موسى ، مصطفى كريم هادي ، مصدر سابق ، ص 489 .

البيانات موضـوع الدعوى عائدة لاشـخاص لهم مسـاس بأمن الدولة ، وهو ما يصـعب من عملية التفتيش على الدليل الرقمية لاثبات واقعة التعدي وانتهاك خصوصية البيانات الشخصية[1].

[1] د. أسـامة غانم العبيدي ، التفتيش عن الدليل الرقمي في الجرائم المعلوماتية ، بحث منشـور في المجلة العربية للدراسـات الأمنية والتدريب ، تصدر عن جامعة نايف العربية للعلوم الأمنية ،المجلد 29 ، 2013 ، العدد 58 ، ص93 .

الفصل الثالث

المسؤولية المترتبة على انتهاك البيانات الشخصية

تكون المسؤولية القانونية متحققة في حال الاعتداء على حق يحميه القانون ، ومن ضمنها البيانات الشخصية التي خصها القانون بحمايته ومنع الغير من الاعتداء عليها ، ورتب احكام المسؤولية القانونية بشقيها المدنية والجزائية ، ولكن بالوقت نفسه سمح في بعض الحالات المتعلقة بمكافحة الارهاب وغسيل الاموال وكذلك في حالة كون طبيعة المعاملة تتطلب الكشف عن هذه البيانات ، وبالتالي سنتناول في هذا الفصل احكام المسؤولية في المبحث الاول وفي الثاني نتناول القيود المترتبة على قيام المسؤولية .

المبحث الأول

احكام المسؤولية القانونية على الشركة المالية

تعرف المسؤولية بشكل عام بأنها محاسبة شخص ما على فعل او امتناع عن فعل ، بمعنى انها جزاء على مخالفة الشخص احد الواجبات الملقاة على عاتقه ، التي تكون بدورها اما واجبات مصدرها القانون او واجبات فرضها المجتمع على الشخص لكونه جزء من المجتمع . فأذا اخل الشخص بالواجب الاجتماعي فأن المسؤولية التي تنشأ هي مسؤولية أدبية ، ولا يتعدى الجزاء على هذا النوع من المسؤولية سوى الاستهجان من جانب المجتمع. فأذا ارتقى الاخلال الى اعتداء أصاب المجتمع فأن المسؤولية التي تنشأ هي المسؤولية الجزائية ، ويكون الجزاء المترتب عليها هو الردع عن طريق إيقاع العقوبة [333] ، اما اذا أصاب الاخلال حق الغير ، فالمسؤولية التي تكون هي المسؤولية المدنية ويكون الجزاء المترتب عليها هو جبر الضرر او التخفيف منه ، وذلك اما بأعادة الحال الى ماكان عليه او بالتعويض عما لحق الغير من ضرر . ولكن ممكن ان يترتب على تصرفات الأشخاص قيام المسؤوليتين الجنائية والمدنية كما في المسؤولية عن الاعتداء على الخصوصية وحماية البيانات الشخصية ، وهنا يحكم على السلوك في المسؤولية الجنائية للعقاب ، ويقرر على السلوك في نطاق المسؤولية التقصيرية التعويض [334] .وعليه سنقسم هذا المبحث الى مطلبين في الأول سنتناول المسؤولية المدنية ، فيما سنتناول في الثاني المسؤولية الجزائية وكالاتي .

المطلب الأول

المسؤولية المدنية التي تترتب على الشركة المالية

ترتكز فكرة المسؤولية المدنية عموما سواء كانت عقدية ام تقصيرية على اركان ثلاثة هي الخطأ والضرر والعلاقة السببية بينهما ، بحيث اذا فقدت المسؤولية المدنية أيا من هذه الأركان انهارت فكرتها ولا يكون هناك محل للتعويض .

---

[333] د. مصطفى العوجي ، القانون الجنائي العام ، ج2 ، المسؤولية الجنائية ، بيروت ، 1985 ، ص11.

[334] د. صبري حمد خاطر ، تطور فكرة المسؤولية التقصيرية ، بحث منشور في مجلة دراسات قانونية ، العدد الأول ، السنة الثالثة ، بيت الحكمة ، بغداد ، 2001 ، ص70 .

والمسؤولية المدنية بدورها تنقسم على قسمين : المسؤولية العقدية وتتحقق اذا امتنع المدين عن تنفيذ التزام عقدي ، او نفذه على وجه معين الحق ضررا بالدائن (كأن يكون هناك عقد بيع ، ثم لا يسلم البائع المبيع الى المشتري فيكون البائع قد اخل بالتسليم) ، اما المسؤولية التقصيرية فتتحق اذا اخل شخص بما فرضه عليه القانون من التزام بعدم الاضرار بالغير ، وهو التزام واحد لا يتغير (كأن يعتدي شخص على مال الغير فيلحق به تلفا ، فيكون هذا الشخص قد اخب بالتزام قانوني عام يملي عليه عدم الاضرار بالغير) وطالما ان هذه الشركات واجب عليها بحكم القانون الالتزام بحفظ بيانات زبائنها ، وحظر اتاحتها للغير الا في حالات معينة ومن بينها إجازة الزبون لذلك ، والاجازة تكون من خلال عقد وبالتالي فأن العقد يحدد الجزاء الذي يترتب على مخالفة بنوده ، وهنا نطبق ما موجود في القواعد العامة في المسؤولية العقدية ولا توجد خصوصية فيه ، ومن خلال ذلك نستبعد فكرة المسؤولية العقدية في اطار هذه الدراسة ، وان المسؤولية التقصيرية هي الحاكمة هنا حيث انها تقوم اذا لم يوجد عقد بين الشركة والزبون ، او قام بينهما عقد باطل او تقرر بطلانه ، او كان هناك عقد صحيح ولكن الاخلال بالالتزام القانوني استوعب الاخلال بالالتزام العقدي كما هو الغالب في مسؤولية الشركة المالية عن حماية البيانات الشخصية لزبائنها .

ولدراسة المسؤولية المدنية عن الاضرار المتحققة بفعل الشركات المالية ، لابد من التعريف بالمسؤولية التقصيرية في الفرع الاول ، وبيان احكامها في الفرع الثاني وكالاتي :

الفرع الأول

التعريف بالمسؤولية التقصيرية المترتبة على الشركات المالية في حالة الاخلال بحماية البيانات الشخصية

يستلزم التعرف على التعريف الكافي للمسؤولية التقصيرية المترتبة على الشركة المالية عن حماية البيانات الشخصية التطرق لتعريفها أولا ومن ثم شروطها ثانيا ، وبيان طبيعتها القانونية ثالثا وكالاتي :

أولا : تعريف المسؤولية التقصيرية : تتحقق اذا اخل شخص بما فرضه القانون من التزام بعدم الاضرار بالغير ، وهو التزام واحد لا يتغير ، كأن يعتدي شخص على مال الغير فيلحق به ضررا ، او يكون هذا الشخص قد اخل بألتزام قانوني عام يملي عليه عدم الاضرار بالغير . ومفهوم المسؤولية التقصيرية لا يوجد فيه ماهو جديد ، ولكن بقدر تعلق الامر بموضوع دراستنا فانه ينبغي الوقوف على معنى المسؤولية التقصيرية الالكترونية . اذ من اللازم بيان مدى اخضاع احكام المسؤولية التقصيرية الناشئة عن اخلال الشركات المالية بالتزامها بحماية بيانات زبائنها الشخصية ومدى اخضاعها للاحكام الناظمة للمسؤولية التقصيرية وفق القواعد العامة ، لان ظهور هذا النوع من الأنشطة أدى الى ظهور نقاط قانونية مستحدثة تحتاج الى البحث والدراسة والوقوف على مدى اخضاعها للقواعد القانونية السارية [335]، وعليه فان الباحث من خلال هذه الدراسة يطرح تساؤلا رئيسيا يتمثل في مدى كفاية التشريعات النافذة حاليا لحكم المسؤوليات الناشئة عن الاستخدام غير المشروع من قبل الشركات المالية لبيانات زبائنها او عدم الحرص على حمايتها والالتزام بالهدف من حفظها ، وهذا التساؤل له ما يبرره فمعظم التشريعات النافذة سنت قبل التحول المفصلي الناتج عن اختراع الحاسوب الالي ، والتزاوج الذي حدث بين تكنولوجيا المعلومات وأدوات الاتصال السلكية

[335] د. سمير حسني المصري ، المسؤولية التقصيرية الناشئة عن استخدام الانترنت ، ط1 ، دار النهضة العربية ، القاهرة ، 2017، ص21 .

اللاسلكية [336]، افرد لنا وليدا اطلق عليه " الانترنت " وحيث ان هناك قواعد عامة للمسؤولية التقصيرية ، فأنه ينبغي التنويه الى ان المقصود بعبارة " القواعد العامة للمسؤولية التقصيرية " في هذا المقام هي القواعد التي تعالج المسؤولية التقصيرية بكافة اقسامها : المسؤولية عن الفعل الشخصي ، والمسؤولية عن فعل الغير ، والمسؤولية عن الأشياء ، وليس فقط القواعد الناظمة لاحكام المسؤولية عن الفعل الشخصي كما درج البعض على ذلك [337]، اذ انه قد ثار الخلاف حول طبيعة المسؤولية الناشئة عن انتهاك القواعد اللازمة لحماية البيانات الشخصية كما سنرى ذلك لاحقا كما يجب الإشارة الى الخلط الذي يحدث لدى البعض بين هذه المسؤولية والمسؤولية في حماية برامج الحاسوب الالي او لما هو منشور على الانترنت على انها دراسات وبحوث سابقة في المسؤولية محل هذه الدراسة . والحقيقة ان هناك فرق شاسع بين هذه وتلك ، فموضوع هذه المسؤولية يتحدث عن مسؤولية مدنية تنشأ نتيجة الاستخدام غير المشروع للحاسوب والانترنت الذي الحق ضررا بالغير ، وعن مدى كفاية التشريعات القائمة حاليا في حكم هذه المسؤولية نظرا لخصوصيتها وتميزها بمجموعة من الميزات غير المتوفرة بالمسؤولية التقليدية ، اذا صحت العبارة . اما العناوين الأخرى المشابهة فهي تتحدث عن كيفية حماية برامج الحاسوب او غيرها من الاعتداء عليها ، هذا وان كان يشكل في جزء منه فعلا ضارا لمالك هذه البرامج وهو ما يدخل في صميم المسؤولية التقصيرية ، ويتداخل مع موضوع هذه المسؤولية محل البحث ، الا ان هناك قوانين خاصة أهمها " قانون حماية حق المؤلف " وفرت هذه الحماية ، وعليه فأن دراستها تخرج أساسا عن القواعد العامة في القانون المدني لتدخل في نطاق قوانين الملكية الفكرية ، ولا يتم الإشارة الى المسؤولية التقصيرية في مثل هذه القوانين الا بكونها طريق استثنائي يمكن اللجوء اليه اذا عجزت هذه القوانين الخاصة عن توفير الحماية المطلوبة ، فبالرجوع الى القانون المدني العراقي المواد (186-232) وكذلك المصري في المواد (163-187) في حين اكتفى المشرع الفرنسي بمعالجة احكام المسؤولية التقصيرية في خمس مواد هي (1382-1386)

ثانيا : اركان المسؤولية التقصيرية للشركات المالية عن اخلالها بحماية البيانات الشخصية لزبائنها .

حسب القاعدة التقليدية في مجال المسؤولية المدنية فان كل خطأ سبب الضرر للغير يلزم محدثه بالتعويض [338] ، ولكن نظرا لخصوصية المجال الذي تستخدم فيه البيانات الشخصية وهو بطبيعة الحال مجال معقد ، الامر الذي يثير التساؤل حول مدى ملائمة الاركان التقليدية للمسؤولية المدنية حتى تنعقد المسؤولية المدنية في هذا المجال وهو ما سنبينه في الاتي :

1- الخطأ : نظرا لما تتمتع به المسؤولية المدنية في اطار حماية البيانات الشخصية من خصوصية تنماز بها عن المسؤولية التقليدية يجب ان يتم بحث ابرز ما يتميز به ركن المسؤولية الأول وهو الخطأ وكالاتي :

أ- مدى ملائمة ركن الخطأ لتحقق المسؤولية المدنية في مجال حماية البيانات الشخصية :

---

[336] د. طارق جمعة السيد راشد ، المسؤولية التقصيرية للناشر الالكتروني عن انتهاك الحقوق المالية للمؤلف ، دار النهضة العربية ، 2012 ، ص34 .

[337] د. طارق جمعة السيد راشد ، المسؤولية التقصيرية للناشر الالكتروني عن انتهاك الحقوق المالية للمؤلف ، مصدر سابق ، ص 36 .

[338] انظر نص المادة 204 من القانون المدني العراقي رقم 40 لسنة 1951 المعدل ، ونص المادة 163 من القانون المدني المصري .

يمكن تعريف الخطأ في مجال حماية البيانات الشخصية بأنه (كل سلوك غير مشروع او مناف للاخلاق او غير مسموح يرتبط بالمعالجة الالية للبيانات او نقلها او انتهاكها) [339]، كما يمكن تعريفه بانه (عمل غير قانوني يستخدم فيه الحاسب الالي كأداة او كموضوع للاعتداء على البيانات الشخصية للمستخدمين) [340].

وعليه فان الخطأ هنا يشمل كل فعل غير مشروع يمثل اعتداء على البيانات في انسيابها وتدفقها بما تمثله من أموال او أصول او اسرار او معلومات شخصية .

وكما رأينا سابقا فان هذه البيانات والمعلومات أصبحت جديرة بالحماية القانونية في الآونة الأخيرة باعتبارها مالا قابلا للتملك او الاستغلال على أساس قيمته الاقتصادية ، وليس على أساس كيانه المادي ، وايا كان الوعاء المادي الذي يتضمنها ، فهي تخول صاحبها ميزتين أساسيتين ، تتمحور الأولى في حقه فضمان سرية بياناته ومعلوماته الشخصية ، بينما تكون الثانية في المطالبة بالتعويض عن الاضرار التي تترتب على أي عمل غير مشروع يقع عليها .

ولا ريب ان وقوع الخطأ كشرط اولي لتحقق المسؤولية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الانترنت ، ثم قيام المخطأ باستخدام الكمبيوتر لكي يحقق له مكنة الاعتداء فيقوم بتحميله برامج وفايروسات واستخدام طرق احتيالية بغية خداعه للدخول الى حسابه ومن ثم إمكانية سرقة بياناته وبيانات حسابه ، او قد يشترك صاحب البيانات بارادته كما هو في البحث موضوع الدراسة ومن ثم تقوم الشركة باستغلال هذه البيانات دون ارادته او خلاف هذه الإرادة [341] .

وقد يتمثل الخطأ في وجود تقصير في مسلك الشركة المعنية بحفظ البيانات ، ما كان ليقع فيه الشخص المعتاد اذا وجد في نفس الظروف الخارجية التي أحاطت بالشركة ، نتيجة تقصير العاملين عليها في القيام بواجب الحيطة والحذر في أداء الاعمال الموكلة اليهم والمتعلقة بهذا الخصوص .

وبناء على ماتقدم يثبت الخطأ في جانب القائم بتجميع البيانات عند ثبوت تقصيره في التزام الأصول المهنية والفنية عند قيامه بعملية التخزين او الحفظ للمعلومات ، ويذهب البعض الى ان من الأصول الفنية التي يجب على المسؤول اتباعها[342] :

- ضرورة توافر الخبرة الدقيقة في كل عمليات تشغيل الحاسوب ، ابتداء من عملية التجميع وانتهاء بعملية التخزين ، واي خلل يقع في احدى العمليات الملقاة على عاتقه يعد ذلك خروجا عن الأصول الواجب اتباعها .
- ضرورة توافر التقنية العالية لدى القائمين على عملية تجميع البيانات ، وتنبيههم على المسؤولية الملقاة على عاتقهم في المحافظة على كافة البيانات والمعلومات المتعلقة بالزبون والتي تتصل بعلمهم ، ومن وصول المتطفلين اليها ، وعدم وضعها بالتداول بدون اذن من صاحبها .

ب- معيار توافر الخطأ عن انتهاك البيانات الشخصية : نظرا لان التقني هو شخص مهني حريص ، وعليه فان العناية التي يجب عليه ان يبذلها في هذا المضمار هي عناية الشخص الحريص ، تتجسد

---

[339] د. محمد سامي الشوا ، ثورة المعلومات وانعكاسها على قانون العقوبات ، ط2 ، دار النهضة العربية ، القاهرة ، 2000 ، ص7 .

[340] د. مصطفى خليف ، مصدر سابق ، ص142 .

[341] في مجال تكنولوجيا المعلومات ، لاشك في ان شراء برامج الاختراق ، ومعدات فك الشفرات وكلمات المرور يمثل جريمة جنائية يعاقب عليها القانون .

[342] د. محمد حسين منصور ، مصدر سابق ، ص363 .

في ضـرورة ان يبذل اقصـى ما في وسـعه للحفاظ على خصـوصـية البيانات الشـخصـية ، كونه متخصصا ومتمكن من تقنيات الحماية المطلوبة لمنع الغير من التعدي على هذه البيانات .

ويرى الباحث من جانبه ان هذا الشخص التقني مطالب بان يبذل درجة عالية من العناية للحيلولة من التعرض لبيانات الزبائن الشـخصـية ، الامر الذي يشـير الى ان المعيار المطالب به التقني هو معيار الرجل الحريص اليقظ ، فأي خطأ في ذكر أي معلومة ولو كانت بسـيطة او تقديم للبيانات مع عدم وجود التزام بالخصـوصـية يعتبر خطأ موجبا للمسـؤولية ، بمجرد قيام دلالة ثابتة وقاطعة في ان عمل التقني يتنافى مع أصـول وقواعد المهنة .

ويتحقق الخطأ في اطار البيانات الشخصية من خلال القيام بتجميع او تخزين للبيانات دون اخطار صاحبها ، وفي ظل انعدام برنامج امني كفيل باحترام كامل لخصوصية المعلومات ، فأن تداولها وانسيابها عبر الانترنت ، وسـهولة الحصـول عليها ولو كانت بطريقة غير مشـروعة ، وكذلك التنافس الشـرس بين الشـركات الكبرى للوصول الى بيانات الزبائن ورصد خصوصياتهم تعد من ابرز صور الخطأ وأكثرها شيوعا [343] .

ت- الأسـاس القانوني للخطأ في حماية البيانات الشـخصـية : نظرا لشـيوع اسـتخدام الانترنت ودخوله في اغلب مفاصـل الحياة اليومية نتيجة لتطور المجتمعات الحديثة والرفاهية التي وصـلت اليها في هذا المضـمار ، مما أدى الى اعتماد الانسـان في نشـاطه اليومي على شبكة الانترنت بصورة كبيرة ، مما زاد في الجانب المقابل في عدد الافراد الذين يتعرضون لآذاها بشكل واسع ، وهو ما يجعل المسؤولية عن هذا النشاط تطرح بشكل حقيقي ، سيما مع خطورة الاضرار التي تسببها .

ونتيجة لكون القواعد العامة في الاثبات تبدو قاصـرة عن توفير الحماية المطلوبة للمضـرور من هذا الفعل ، وخصـوصـا اذا لم يتمكن من اثبات سبب الحادث ، واذا تمكن من اثباته فقد يتعذر عليه اثبات تحديد المسبب ، مما يحول دون حصـول المتضرر على حقه في التعويض ، فهل نجد في نظرية المسؤولية الشيئية جوابا وافيا ، فهي مسـؤولية لا تقوم على الخطأ المفترض وانما تقوم على ملكية الشـيئ الذي احدث الضـرر ، وتجعل المالك مسؤولا عن مخاطر ملكه ، وذلك على أساس تحمل تبعة المخاطر ؟.

فمن خلال موقف القانون المدني العراقي يتضـح بأن المشـرع لم يجعل المسـؤولية مفترضـة بخصـوص جميع الأشياء غير الحية ، وانما حدد المسؤولية المفترضـة على الأشياء التي تتطلب حراستها عناية خاصـة ، سواء بسـبب طبيعتها او بالنظر لما يحيطها من الظروف والملابسـات التي تجعلها مصـدرا لخطر يلزم له عناية وحرص خاص ، وهو المتحقق في مجال حماية البيانات الشخصية لزبائن الشركات المالية .

ويمكن الاخذ بنظرية الحراسة القانونية ، التي تقرن الحراسة بحق الملكية لشخص على الشيء محدث الضرر ، فالحارس هنا هو من له حق الملكية .

والحارس هو من تثبت له السلطة القانونية على الشـيء والتي يستمدها من حق عيني على الشـيء او من حق شخصـي متعلق به ، ومصدر هذه السلطة يكون العقد او نص القانون او الإرادة المنفردة [344] .

ووفقا لتلك النظرية فان المسؤول عن الفعل الضار للبيانات الشخصية هو من يملك السيطرة القانونية والفعلية على طريقة تداول تلك البيانات عبر الانترنت ، أي من يملكها ، ومع ذلك ينهض سؤال هنا هو من يعد المالك هل هي الشركة ام الزبون الذي انتقلت اليه ملكية حسابه بمجرد التسجيل والاشتراك ؟.

وفقا للوضـع الطبيعي للامور فان الزبون على الرغم من تسـجيل بياناته ودخوله في برنامج الشـركة واعتباره بذلك الحائز المادي لحسـابه في الشـركة المالية مثلا ، ومن ثم صـاحب جميع السـلطات عليه وخصـوصـا اذا

---

[343] د. محمد حسين منصور ، المصدر السابق ، ص367.

[344] د. احمد شوقي عبد الرحمن ، مسئولية المتبوع باعتباره حارسا ، دار الفكر العربي ، القاهرة ، 1998 ، ص58 .

ماتسلم كلمة المرور او الرقم السري للدخول ، بيد انه الطرف الذي لحقه الضرر ، ومن ثم فأن المسؤول عن الخطأ هو الذي انتهك خصوصية البيانات الشخصية ويتوقف تحديده على ما اذا كان خطأ اداري او خطأ فني ، ففي حالة الخطأ الفني تقع المسؤولية على عاتق متعهد الايواء او مورد البيانات ، كما يعد اهمال او تقصير المسؤول في هذه الحالة عن الصيانة سببا لقيام المسؤولية ، وعلى صعيد اختراق قواعد الخصوصية وانتهاك سرية البيانات الشخصية الخاصة فان المسؤولية تنعقد على المعتدي ، اما في حالة الخطأ الإداري وحالة ثبوت التقصير في اتخاذ الاحتياطات التقنية اللازمة فان المسؤول هي الشركة او صاحب السلطة الفعلية في هذه الشركة .

لكن التحديد السابق قد يؤدي الى بعض الإشكاليات القانونية ، اذ ان إمكانية تحديد اركان المسؤولية وفقا لما مر ذكره امرا بالغ الصعوبة ، فحتى لو تم تحديد طبيعة الاخطار وتقدير الاضرار المترتبة عليها ، فان تحديد الشخص المسؤول عن انتهاك السرية من بين جميع الأشخاص الممكن ان يكونوا هم ليس بالامر السهل ، فاي منهم تكون له صفة الحارس الذي يمكن الرجوع عليه بالتعويض حال انتهاك سرية البيانات الشخصية وهو ما سنحاول بيانه في تحديد الحارس المسؤول (في حالة تعدد الحراس) ، اذ يتعدد حراس الشيء في احد الفرضين : أولهما هو فرض تجزئة الحراس الذي يتولى فيه الحراسة على الشيء هو الشركة باعتبارها مالك الموقع او منشئ الموقع الالكتروني او مورد البيانات او متعهد الايواء وهما من تنتقل اليهما سلطة الرقابة والتوجيه باعتبار أي منهما حارسا للاستعمال ، اما الفرض الثاني وهو تعدد الحراس في اطار حراسة التكوين ذاتها :

الفرض الأول : افتراض مسؤولية منشئ الموقع في الفرض الخاص بتجزئة الحراسة . مما لا شك فيه ان نظرية تجزئة الحراسة نشأت في الأصل بهدف تخفيف مسؤولية الحارس غير المالك الذي عهد اليه بالشيء للاستخدام المؤقت ، دون ان تكون له سلطة فعلية فيما يخص مكوناته الداخلية .

وفيما يتعلق بمجال خصوصية البيانات الشخصية ، يمكن ان يكون تعيين الشركة او منشئ الموقع حارسا لهذه البيانات ، وتحمله وحده المسؤولية حال انتهاك سرية البيانات الشخصية فيه الكثير من الاجحاف والعنت ، حيث لا يستطيع في اغلب الأحيان ان يتلافى التدخل الضار لغيره من الأشخاص .

وبخصوص ذلك يطرح التساؤل بسأن تحديد الحارس الذي يرجع الضرر الى خطأه ، هل هو حارس التكوين (مالك الموقع "الشركة" منشئ الموقع) او حارس الاستعمال (مورد المعلومات ، متعهد الايواء).

لاريب انه في الحالة التي تبدو فيها عيوب اختراق سرية البيانات الشخصية ظاهرة او يسهل استخلاصها من ظروف الحال ، بحيث يسهل ارجاع التعرض للبيانات اما الى العيب التقني الداخلي لإجراءات الأمان او التطبيق الالكتروني ، وبناء عليه يسهل اثبات خطأ الشركة المالكة للموقع او مؤسسه باعتباره حارسا للتكوين ، او ارجاع سبب الاختراق الى المسلك الخارجي المتمثل في إدارة نقل وتبادل المعلومات ، مما يعني اسناد الخطأ الى تقصير من يتولى حراسة الاستعمال [345].

بيد ان الصعوبة تبدو في الحالة التي يتعذر فيها تحديد سبب انتهاك البيانات الشخصية او الطريقة التي تم من خلالها اختراق التطبيق او الموقع ، ومن ثم تحديد المسؤول ، وقد يكون الوضع الطبيعي هو رفع الدعوى على كلا الحارسين وترك الامر للقضاء للنظر فيه في اطار الخبرة الفنية [346] . الا انه لا يخفى مايمكن ان

---

[345] Goldman (B.), La determination du garden responsible du fait des choses inanimees, these, Lyon, 1945,p.12.

[346] د. حسن جميعي ، مسئولية المنتج عن الاضرار التي تسببها منتجاته المعيبة ، دار النهضة العربية ، القاهرة ، 2000 ، ص159 .

يترتب على هذا الامر من نتائج قد يكون من اكثرها ايلاما على المضرور المدعي ان ترفض دعواه على كلا الحارسين ، إضافة الى ما يمكن ان يمثله ذلك من تكاليف مالية وجهد مضاعف مما يضر بالمضرور ، لذلك فان مصلحة المدعي تقتضي ان تبقى مسؤولية مالك الموقع (الشركة المالية) او منشأه مفترضة باعتباره حارسا للتكوين حتى في الحالات التي تكون فيها الاضرار عن التقرير في الرقابة على سرية تبادل البيانات ، بوصفه الاقدر على الاشراف والرقابة على الموقع او البرنامج الالكتروني الذي أدخلت اليه بيانات الزبون الشخصية ، وحتى في الحالات التي يصعب فيها تحديد وسيلة او سبب انتهاك سرية البيانات الشخصية .

الفرض الثاني : تحديد حارس التكوين في الفرض الخاص بتعدد وسطاء الانترنت : بما ان التخصص هو الضابط الحقيقي للتعامل مع البيانات الشخصية ، بحيث اصبح التعامل مع التقنيات الحديثة في المجال التكنولوجي تحتاج الى نوع من التخصص في التكوين والصيانة والبرمجة والإدارة ، اذ لم يعد متصورا حاليا ان ينفرد شخص واحد بإدارة عمليات نقل البيانات عبر الشبكة العنكبوتية ، فمن المؤكد ان هناك متخصصين في ابتكار التطبيقات والمواقع الالكترونية ، وهناك متخصصين في الإدارة ، ومتخصصين في انشاء تقنيات الارسال ، ومتخصصين في الاشراف على عمليات نقل البيانات ، ومتخصصين في التطوير ، وأيضا ان هناك متخصصين في الصيانة وإصلاح الأعطال .

وبناء على ذلك اذا حدثت أي من صور انتهاك البيانات السابق الإشارة لها نتيجة وجود خلل في تقنيات نقل وتبادل البيانات والمعلومات ، يثور السؤال عمن هو الذي يعد حارسا للتكوين هنا ، ويلتزم بناء على ذلك بتعويض الضرر الناشئ عن انتهاك خصوصية البيانات او التعدي عليها ؟.

ليست هناك ثمة مشكلة اذا امكن تحديد نقطة الخلل التي سهلت التعدي ، فقد يكون سبب الخلل عيب في تقنية انشاء الموقع ذاته حيث تنعقد مسؤولية المؤسس او المالك نفسه ، او يكون الخلل لعيب في تقنيات الارسال فتتحقق مسؤولية وسيط الارسال ، او خلل في رقابة وتأمين ونقل وتبادل البيانات ، فتنعقد مسؤولية متعهد الايواء.

ولكن توجد الصعوبة في الحالة التي لا يمكن فيها تحديد النقطة التي أدت الى حدوث التعدي ، حيث يرى الباحث الرجوع على جميع الأشخاص الذين تثبت لهم صفة حارس التكوين للموقع على سبيل التضامن ، واذا تعذر الرجوع عليهم مجتمعين نظرا لضعف الإمكانيات المادية والفنية للزبون المعتدى على بياناته الشخصية ، ونظرا الى ان محل الاعتداء وهو الشبكة الدولية للانترنت والتي يكون مشئيها ووسطائها منتمون لدول عدة ، إضافة للشركة المالية ذاتها ، مما يصعب علي المتضرر الرجوع عليهم مجتمعين ، فيكون رفع الدعوى على مالك الشركة والتي يكون موطنها محددا، كونه الحارس الظاهر امام زبائنها . مستخدمي مواقعها وتطبيقاتها الالكترونية .

وبمجرد ان يثبت ان ثمة خلل في وظائف الأمان الالكتروني كان السبب في انتهاك سرية البيانات الشخصية للزبون ، فانه يجب على القضاء ان يفترض مباشرة مسؤولية مؤسس الموقع ومالكه على أساس الخطأ في الحراسة وفقا لقواعد المسؤولية الشيئية .

ويعد هذا المسلك بشأن اثبات علاقة السببية في مجال حراسة التكوين للمواقع الالكترونية ، متماشيا مع المبادئ الأساسية الحاكمة لمسؤولية الحراسة عن الأشياء ، حيث انه قد وقع التعدي والضرر على البيانات بسبب الخلل في أي من تقنيات الموقع الالكتروني ، فان الزبون المتضرر يجب الا يقع على عاتقه إقامة الدليل على علاقة السببية بين مالحقه من ضرر نتيجة انتهاك خصوصية بياناته وبين خلل الموقع الالكتروني او خطأ المؤسس [347].

[347] د. حسن جميعي ، مصدر سابق ، ص169 .

لكن يجب الإشارة الى انه بالرغم من القرينة القضائية التي تكون بمجرد حدوث اختراق للبيانات الشخصية في هذا الفرض اسوة بالقرينة التي يقيمها القضاء لصالح المتضرر من فعل المنتجات المعيبة ، فان المؤسس او المالك او وسيط الشبكة او المدير يمكنه ان يدفع مسؤوليته اذا اثبت اتخاذه لكافة وسائل الأمان والاحتياط اللازمة لمنع اختراق تطبيقه الالكتروني ، وان عملية الاختراق التي حدثت سببها خطأ الزبون نفسه الذي سهل دخول الغير لحسابه او عبر نشر بياناته وجعلها مباحة للاطلاع عليها من قبل العامة ، او حال اثبات السبب الأجنبي .

2- الضرر : يلزم ثانيا لتحقق المسؤولية المدنية عن الاضرار التي تصيب البيانات الشخصية لزبائن الشركات المالية حدوث ضرر لاصحاب هذه البيانات ، فما هو المقصود بالضرر هنا وما هي شروطه؟.

أ- المقصود بالضرر وصوره : يعرف الضرر بصورة عامة بانه " الاخلال بحق او مصلحة ذات قيمة مالية للمتضرر " [348]، كما عرف بانه " مايصيب الشخص في حق من حقوقه او بمصلحة مشروعة له " [349]. واصبح المستقر عليه انه طالما كانت المصلحة مشروعة ، فيستوي بعد ذلك ان تتعلق بسلامة جسده او بماله او بشرفه او بعاطفته او بحريته او في أي مصلحة يحرص عليها الشخص .

وينقسم الضرر وفقا للوضع الطبيعي الى ضرر مادي يصيب الذمة المالية للمتضرر ، وضرر معنوي يتمثل في المعاناة والالام التي تصيب شعور المتضرر او عاطفته ، ولم يعد هناك خلاف في الفقه بين شمول التعويض لكلا النوعين من الضرر .

ولا ريب في تحقق كلا النوعان من الضرر للمعتدى على بياناته الشخصية وعلى خصوصياته ، فالدخول الى المواقع الالكترونية بما فيها من بيانات ومعلومات سرية يتم بسهولة وسرعة ، ويكون الضرر الناجم عن الاطلاع والكشف على الأمور السرية والبيانات الشخصية بمثابة انتهاك لخصوصية صاحب الحساب ، الامر الذي قد يلحق به العديد من الاضرار المادية الناتجة عن كشف بياناته ومعلوماته عبر الانترنت ، اذ يكون هناك عدد غير محدود من المطلعين عليها ، وهو مايصيبه باضرار بالغة تتمثل في خسارته لبعض أمواله نتيجة سرقة كلمات مروره السرية لحساباته البنكية والحصول على أموال من حساباته او غيرها من الاضرار [350] .

كما يتمثل الضرر الادبي الناشئ عن انتهاك السرية والاعتداء على البيانات الشخصية في انتهاك حرمة الحياة الخاصة للزبائن ، وما يستتبعه ذلك من المساس بسمعة الشخص الاجتماعية ونشر معلوماته واسراره الخاصة ، بما قد يحتوي من تجريح واهانة وفضح لاسراره وصوره او لمعلوماته الاجتماعية او الصحية [351].

---

[348] د. عبد الرزاق احمد السنهوري ، الوسيط في المسئولية المدنية ، الجزء الأول ، الفقرة 571 ، ص856 .

[349] د. سليمان مرقس ، الوافي في شرح القانون المدني ، الفعل الضار ، ط7 ، الجزء الثالث ، زين الحقوقية ، بيروت ، 2019 ، ص133 .

[350] د. منصور بن صالح السلمي ، المسئولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي ، جامعة نايف للعلوم الأمنية ، الرياض ، 2010 ، ص103.

[351] في سياق ذلك وفي عام 2014 ايدت محكمة استئناف عمان قرارا صادرا من محكمة بداءة حقوق عمان بتعويض المشتكي مبلغ وقدره 12500 دينار اردني ، يدفعها المدعى عليه بعد قيامه بنشر صورة زوجة المدعي عارية عبر مواقع التواصل الاجتماعي ، مما أدى الى تطليق هذه الزوجة واصابتها بالضرر المعنوي الجسيم ، كما قضت المحكمة للمدعي بمبلغ 10 الاف دينار بدلا لاضرار معنوية لحقت به حيث اثر ذلك على سمعته وشرفه ومركزه المالي مما اضطره لترك وظيفته ومغادرة محل عمله في الامارات ، انظر مقال منشور بعنوان الجرائم الالكترونية عبر الفيسبوك ، الأدلة والثغرات والتعويض ، عبر الموقع الالكتروني التالي

https://www.7iber.com/society/facebook-cyber-crimes.

ب- شروط الضرر : يشترط في الضرر الذي يستلزم التعويض ضرورة ان يكون محققا ، أي ان يكون قد وحصـــل بالفعل ، او ان وقوعه مســـتقبلا امر حتمي ، وهو ما يتوفر بلا ادنى شـــك في الضـــرر المعلوماتي الناشـئ عن الاعتداء على البيانات الشـخصـية فهو دائما محقق ، اذ ان الضـرر الاحتمالي غير متصور على صعيد انتهاك السرية المعلوماتية ، فمجرد حدوث الاعتداء على البيانات والاطلاع على البيانات الشـخصـية للزبون وهو في حد ذاته ضـررا محققا ، بغض النظر عن الاضـرار التي ممكن ان تتبع الاعتداء .

كما ويشترط ثانيا في الضرر ان يصيب مصلحة مشروعة للمتضرر ، الامر المتحقق أيضا بالنسبة للاعتداء الذي تعرض له الزبون ، حيث ان حرمة بياناته الشخصية وخصوصياته تعتبر من اهم المصالح المشروعة للأشخاص والتي يجب على الشركات المالية ان توفر لها الحماية القانونية .

ويلزم في الضـــرر ثالثا ان يكون مباشـــرا ، اذ ان الضـــرر المباشـــر وحده الذي يتم التعويض عنه في اطار المسؤولية المدنية ، ويكون الضـرر مباشـر اذا كان نتيجة طبيعية للاعتداء ، ولم يكن في الإمكان منع حدوثه بجهد معقول ، الامر الموجود كذلك في الضرر الناشئ عن التعدي على البيانات الشخصية .

3- علاقة السببية : إضـافة للخطأ والضـرر كاركان لقيام المسؤولية المدنية يسـتلزم القانون وجود العلاقة السببية بين الخطأ الذي بموجبه تم الاعتداء على خصوصية المعلومات الزبون وبياناته الشخصية وبين الضرر الحاصل .

وبخصـوص اثبات الرابطة السببية فيمكن القول بأنه وان كان يصـعب على المتضـرر إقامة الدليل على الخطأ الذي ترتكز عليه المسؤولية ، نظرا لصـعوبة تمييز الخطأ وقت حدوثه او تحديد مصـدره نظرا لتعدد مراحل وقوع الامر الالكتروني بالاعتداء [352] . لكن وبســهولة يمكن ارجاع الضــرر المتحقق الى هذا الخطأ واثبات العلاقة السـببية بينهم ، فلا يوجد سـبب اخر لاختراق خصـوصـية البيانات الشـخصـية بدون علم صـاحبها او اسـتغلالها دون سـابق معرفة او إجازة منه ، وان ظلت قضـية تحديد هوية مرتكب فعل الاعتداء مثار صـعوبة وبالتالي يمكن الرجوع على من تثبت له الحراسة كما سبق بيانه .

الفرع الثاني

حكم تحقق المسؤولية التقصيرية

من المسلم به ان لكل شخص تعرض لضرر مادي او ادبي المطالبة بالتعويض ، وهو جزاء المسؤولية المدنية ، وبقدر تعلق الامر بصاحب البيانات الشخصية فان يملك الحق في المطالبة بالتعويض عن الاضرار او الالام الناتجة عن مخالفة القواعد الخاصة بحماية البيانات التي نصت عليها القوانين المعنية [353] .

وان القوانين التي نظمت القواعد الخاصـة بحماية البيانات الشـخصـية للأشـخاص الطبيعيين وبقدر تعلق الامر بتجهيز ومعالجة البيانات الشخصية تبنت نهجا واسعا لتعويض الاضرار من حيث أساس المسؤولية وطرق التعويض ، فمن الممكن المطالبة بالتعويض عن كافة الخســـائر الناجمة عن الخروج على احكام هذه القوانين [354].

---

[352] د. منصور بن صالح السلمي ، مصدر سابق ، ص111.

[353] انظر نص المادة 82 من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016 .

[354] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، مصدر سابق ، ص434

وبطبيعة الحال يشترط للحكم بالتعويض ان يكون هناك اعتداء على البيانات الشخصية الذي يسبب عادة ضررا حقيقيا يتمثل في انتهاك الخصوصية ، فالبيانات والمعلومات التي يتم تجميعها ومعالجتها لابد وان يكون لهدف واضح ومحدد سلفا ، ولابد من التزام الشركات بالهدف الذي من اجله قامت بتجميع تلك البيانات ومعالجتها ، مما يعني اذا تجاوزت هذا الهدف فلا مناص من الرجوع عليها بدعوى المسؤولية [355] .

كما تخضع العديد من البيانات الشخصية والمعلومات المتاحة للمعالجة للسرية ، ويفرض هذا التزاما قانونيا او تعاقديا يتمثل في ان أي افشاء للبيانات او المعلومات سيترتب عليه مسؤولية قانونية ، مع ما قد ينص عليه العقد من اثار قد تتمثل في توقيع الجزاءات المنصوص عليها في العقد او حتى انهاءه من جانب المتعاقد المضرور (صاحب البيانات) حماية للخصوصية التي هي على المحك في حالة انتهاك المعلومات الشخصية المتعلقة بالزبائن او حتى العمال [356] .

وعلى الرغم من اثارة مسؤولية الشركات التي تتعامل بالبيانات الشخصية وفقا للتشريعات المقارنة ، لقيامها بالحاق الضرر المادي او المعنوي بالزبون صاحب البيانات ، الا انها تبدو امرا في غاية الصعوبة من الناحية العملية ، ذلك ان ملاحقة المسؤول عن الضرر يستلزم تحديد هويته ، ثم تحديد الاضرار التي تسبب بفعله في احداثها .

لذلك ومن وجهة نظر الباحث فان هذا الامر وكما بيناه سابقا يعد وبحق انعكاسا صادقا لعمق مشكلة الممارسات غير المشروعة التي تقع على البيانات الشخصية ، لما تمثله من تهديد حقيقي لحقوق جديرة بالحماية ، اذ ليس بخاف ان العديد من القائمين بجمع البيانات الشخصية ومعالجتها قد قاموا باستغلال البيانات الشخصية في الدعاية التجارية ، او المساس بحرمة الحياة الخاصة [357] .

ويمكن ان نستخلص من الموقف التشريعي الناظم للمسؤولية والتعويض فيما يتعلق بالاعتداء على البيانات الشخصية المبادئ الاتية :

أولا : تبني مبدأ المسؤولية المشروطة : يتضح من نص المادة (82) من اللائحة الاوربية السالفة الذكر ان المشرع الأوربي تبنى نهجا تشريعيا قائم على مبدأ التوازن بين مصلحة الشركة من جهة وعدم تحميلها بالتزامات او أعباء مرهقة ، وحماية أصحاب البيانات الشخصية من جهة أخرى .

فالاصل هنا هو عدم مسؤولية الشركة عن أي ضرر يلحق بصاحب البيانات عن الاضرار التي لحقت به نتيجة معالجة البيانات ، هذه البيانات الحساسة الخاصة به طالما انها التزمت بكافة الالتزامات التي نص عليها القانون ، لان الأصل العام هو حظر جمع او معالجة هذه البيانات ، الا ان الشخص المعني يستطيع عن طريق الرضاء الصحيح ان يرخص بذلك وهنا تصبح المعالجة التي تقع على هذه البيانات امرا مشروعا ، ولا يتعارض مع احكام الخصوصية [358] .

---

[355] د. طارق جمعة السيد راشد ، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، مصدر سابق ، ص137 .

[356] د. باسم محمد فاضل مدبولي ، مصدر سابق ، ص 151 .

[357] د. طارق جمعة السيد راشد ، مصدر سابق ، ص 44 .

[358] انظر نص المادة (a/2/9) من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .

وينسجم مبدأ المسؤولية المشروطة مع موقف القوانين الذاهب الى مسؤولية الشركة عن تعويض الاضرار التي تلحق بالشخص المعني في الحالة التي لا تمتثل فيها للالتزامات المنصوص عليها في القوانين الخاصة بجمع ومعالجة ونقل البيانات الشخصية للزبائن .

ثانيا : اثر الاخذ بفكرة الخطأ – فرض التزامات محددة على الشركة

يقتضي تأسيس مسؤولية الشركة على فكرة الخطأ ان تكون هناك التزامات محددة كما اسلفنا ، لان توفر الخطأ يفترض الاخلال بالتزام محدد ، وقد حصرت بعض التشريعات هذه الالتزامات تحت مسمى المبادئ الحاكمة لعملية جمع ومعالجة البيانات الشخصية كما في اللائحة الاوربية .

ومن بين اهم الالتزامات التي اشارت اليها اللائحة الاوربية هو التعاون مع السلطات المختصة باخطارها بحدوث انتهاك للبيانات الشخصية .

ووفقا لهذا الالتزام يجب على مراقب البيانات او المتحكم في الشركة ان يقوم دون تأخير مبرر في موعد لا يتجاوز اثنين وسبعين ساعة من علمه بحدوث انتهاك للبيانات الشخصية ان يقوم باخطار السلطة المشرفة المختصة بهذا الانتهاك [359] ، وقد حدد القانون مواصفات الاخطار [360].

ولكن اذا كانت الشركة ملتزمة بتزويد السلطات العامة بأية خروقات للبيانات الشخصية شاملة على الوقائع المتعلقة بانتهاك البيانات الشخصية واثارها والإجراءات التصحيحية المتخذة ، فأن التساؤل يثور عما اذا كان من الجائز لغير السلطات وتحديدا المضرور ان يلزم الشركة بالكشف عن هوية المخطئ ام لا .

للإجابة على هذا السؤال يرى الباحث انه لايجوز الزام الشركة بالكشف عن الشخص المخطئ الا وفقا لضوابط وإجراءات محددة تضمن سرية المعلومات ، ولا ينال من سلامة هذا النظر كون اللائحة الاوربية لم تتعرض سوى لاخطار السلطات المختصة ، لأننا لو كنا نسلم بحق المضرور بالزام الشركة بإزالة الضرر وتعويض الشخص المعني في حالة عدم التزامها بالاشتراطات التي نص عليها القانون ، فلماذا لا نجيز له ان يطلب الكشف عن هوية مرتكب الفعل الضار او سبب الانتهاك عندما تكون عدم المشروعية ظاهرة .

ثالثا : القاعدة العامة مبدأ التعويض الكامل والعادل للمضرور : من المبادئ التي اعتمدتها القوانين الناظمة لحماية البيانات الشخصية [361]، مبدأ التعويض الكامل للاضرار المادية والمعنوية التي تنشأ نتيجة انتهاك الشركة لاحكام القانون [362] .

---

[359] انظر نص المادة (1/33) من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016 .

[360] نصت المادة (3/33) من اللائحة على انه يجب ان يتضمن البلاغ على الأقل البيانات الاتي :

a- وصف لنوع الخرق لحماية البيانات الشخصية وفي حال كان ممكنا الفئة والعدد التقريبي للأشخاص المعنيين بهذه البيانات وفئتهم والعدد التقريبي لسجلات البيانات الشخصية المتعرضة للخرق .
b- أسماء وبيانات الاتصال الخاصة بمفوض حماية البيانات او نقطة تواصل أخرى للحصول على معلومات إضافية.
c- وصف للتبعات المحتملة لخرق حماية البيانات الشخصية .
d- وصف للتدابير التي اتخذها او يوصي باتخاذها لتصحيح هذا الخرق للبيانات الشخصية والتدابير لتخفيف الاثار الضارة المحتملة .

[361] انظر نص المادة (1/82) من اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لسنة 2016.

[362] د. عبد الصادق محمد سامي ، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية ، مصدر سابق، ص 64 .

ويعد انتهاك الخصوصية مناطا للتعويض بصرف النظر عن توافر الخطأ من عدمه ، فاذا تحقق الضرر وجب التعويض عن كافة عناصره بحيث يعوض عن الضرر ولا شيء غير الضرر وفقا لمبدأ التعويض الكامل الذي يمنع ان يثرى المضرور من التعويض ، ويشمل التعويض مالحقه من خسارة وما فاته من كسب .

ومن اللازم الإشارة الى ان الاعتداء على الحياة الخاصة بسبب خطأ الشركة يمكن ان ينشأ عنه ضرر مادي يتمثل في الخسارة التي تلحق بمن انتهكت خصوصياته او الكسب الذي يفوت جراء الاعتداء ، غير ان هذه الاضرار تبقى قليلة مقارنة بالاضرار الأدبية التي تحدث في هذا الاطار [363] .

كما يجب ان يكون التعويض عادلا ، ولن يكون كذلك الا اذا كان تقدير الاضرار عادلا [364] ، ومن العناصر التي يجب ان تؤخذ في الاعتبار استخدام البيانات الشخصية في الإعلانات والدعاية التجارية .

ويستحق الشخص المعني مقابلا عادلا عن الاعتداء على بياناته الشخصية ، حتى ولو كان قد اعطى الاذن بمعالجة بياناته ، لانه مما لا شك فيه ان إساءة استخدام البيانات يساهم بشكل كبير في انتهاك الخصوصية كما ان البيانات والمعلومات التي يتم تجميعها ومعالجتها لابد وان تكون لها هدف واضح ومحدد سلفا ولابد من التزام الشركة بالهدف الذي من اجله قامت بتجميع هذه البيانات ومعالجتها .

ولما لما كان اثبات مقدار الضرر الفعلي امرا صعبا فأن القضاء يلجأ الى التقدير الجزافي للضرر ، لانسجامه مع اعتبارات العدالة خاصة في ظل عدم وجود تقدير محدد . ويراعى في هذا التقدير ان يكون كافيا بالقدر الذي لا تحقق مع الشركة أي ميزة مالية من الاعتداء غير المشروع على البيانات الشخصية ، كما يجب ان تراعى الاعتبارات الخاصة بالمضرور المعتدى على بياناته الشخصية ، واهمها مركزه الاجتماعي والثقافي والعلمي والفني والاقتصادي ، ومدى تاثير الاعتداء على سمعته .

واذا كان تقدير التعويض عن الضرر المادي يبدو سهلا فان الامر لا يبدو كذلك بالنسبة للضرر المعنوي الناتج عن الاعتداء على البيانات الشخصية ، وذلك لما تتسم به هذه البيانات من طابع غير ملموس يتعلق بسمعة الشخص واعتباره ، فضلا عما يسببه اجتماع الضررين المادي والمعنوي من صعوبة في تقدير التعويض المالي ، ولذلك يتم عادة دمجهما وتقدير التعويض عنهما دون تخصيص [365] .

ويرى الباحث انه يجب الا يقتصر القاضي عند تقديره لمقدار التعويض على ما لحق المضرور من خسارة وما فاته من كسب ، ولكن يجب ضرورة الاخذ في الاعتبار الأرباح التي جنتها الشركة من فعل الاعتداء.

أيضا يجب ان يلزم المشرع القاضي بقواعد خاصة لتقدير التعويض من خلال الاعتداد بجميع عناصر الضرر على نحو مفصل ، وهو ما يحقق العدالة ويفضي الى ارتفاع مقدار التعويض المحكوم فيه ، ويؤدي بطبيعة الحال الى ردع الشركات او الشخص المسؤول عن الضرر من معاودة الاخلال بأحكام القانون اثناء التعامل مع بيانات الزبائن الشخصية ، مع الوضع في الاعتبار ان المقصود من ذلك ليس تقنين فكرة التعويض العقابي في هذا الصدد ، لان الأساس الذي تقوم عليه قواعد المسؤولية بالدرجة الأولى هو تعويض المضرور لا معاقبة المسؤول ، فالتعويض اذا يقاس بمقدار الضرر الذي أصاب المضرور بالذات حسب الأصل وخاصة

---

[363] د. سيد اشرف جابر ، مسؤولية مقدمي خدمات الانترنت عن المضمون الالكتروني غير المشروع ، دار النهضة العربية ، القاهرة ، 2010 ، ص184 .

[364] د. جميل الشرقاوي ، النظرية العامة للالتزام ، الكتاب الأول ، مصادر الالتزام ،دار النهضة العربية ، القاهرة ، 1995 ، ص 478 .

[365] د. سيد اشرف جابر ، مصدر سابق ، ص 188 .

الاثار المالية المترتبة على وقوع الضرر حيث تختلف من شخص لاخر ، فالتعويض يقدر بحسب الظروف الشخصية للمضرور وليس تقديرا مجردا [366].

ويرى البعض ان هذه الطريقة في حساب التعويض تعد الأفضل في تحقيق العدالة على وجه الخصوص في مجال البيئة الرقمية ، حيث تساهم هذه الأخيرة في انتشار الضرر الذي يصيب المضرور على نطاق واسع ، بسبب زيادة حجم المنضمين لها ، وبالتالي فاذا كانت الشركة قد استفادت من تحقيق المزيد من الأرباح ، فيجب ان يأتي التعويض ليحرمها من كل الأرباح التي جنتها بصورة غير مشروعة [367]، وهو ما يراه الباحث كذلك .

رابعا : مبدأ التعويض الفعال للمضرور عن طريق فكرة الحلول :

يبدو ان المعالجة التشريعية الخاصة بحماية البيانات الشخصية تذهب باتجاه تبني نظام التعويض الفعال للمضرور ويتضح ذلك من خلال الحصول على التعويض الكامل من الشركة او من الشخص المخطئ سواء كان القائم بالمعالجة او المتحكم بالبيانات حال اشتراك اكثر من وحدة تحكم او اكثر في احداث الضرر للشخص المعني .

وهذا ليس فرضا نظريا بحتا ، بل يفرضه واقع ما نصت عليه القوانين المرعية [368] ، ويبدو ان هذا النهج الخاص بتعويض الاضرار يقضي بان يتم صرف التعويض مباشرة من خلال قيام الشركة بدفع تعويض كامل عن الضرر المتكبد ، على ان تقوم الشركة لاحقا بالرجوع على أي مسؤول اخر سواء كان متحكما في البيانات او معالجا بمبلغ التعويض الخاص بيهم كجزء من مسؤوليتهم عن الضرر ووفقا لقاعدة مسؤولية المتبوع عن اعمال تابعيه [369].

وتبرز فكرة فاعلية التعويض عن انتهاك البيانات الشخصية او الاخلال بالالتزامات التي اقرتها القوانين اثناء التعامل مع بيانات الزبائن في ان عملية تعويض المضرور عن الاضرار التي تصيبه تمثل الهدف الاسمى للتوجه التشريعي الجديد ، فأيا كانت أهمية الالتزامات التي يخالفها فاعل الضرر ، فان المحصلة النهائية لهذه المخالفة هي الحكم بالتعويض على المسؤول [370].

وعلى الرغم من ان المشرع الأوربي نص في لائحته على مسألة فاعلية التعويض الا انها لم تنص على الية واضحة ومحددة او طريقة تضمن سرعة تحقيق الوظيفة التعويضية لحصول المضرور على التعويض الكافي لاشباع حاجته في الشعور بالأمان والعدالة في المجتمع الذي يعيش فيه باستثناء فكرة الحلول التي نص عليها في محاولة منه لايجاد وسيلة فاعلة وسريعة لحصول المضرور على التعويض .

---

[366] د. علاء عيد طه ، الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها ، أطروحة دكتوراه مقدمة الى كلية الشرق العربي للدراسات العليا في الرياض ، 2018 ، ص183 .

[367] د. عبد الهادي فوزي العوضي ، المسؤولية التقصيرية لناشري برامج التبادل غير المشروع للمصنفات الفكرية ، دار النهضة العربية ، القاهرة ، 2016 ، ص 164 .

[368] اذ نصت الفقرة الرابعة من المادة 82 من اللائحة الاوربية العامة لحماية البيانات الشخصية (GDPR) على انه " في الحالات التي تشترك فيها اكثر من وحدة تحكم واحدة او اكثر من معالج ، او كل من المتحكم والمعالج في نفس المعالجة وحيثما تكون بموجب الفقرتين الثانية والثالثة مسؤولة عن أي ضرر ناجم عن المعالجة ، ويتحمل كل متحكم او معالج المسؤولية عن الضرر بأكمله من اجل ضمان التعويض الفعال للشخص المعني صاحب البيانات "

[369] Suzanne Carval , Patrice Jourdain , Genevieve Viney : Les effets de Ia responsabilite 4e edition , Editeur : L . G . D . J , 2017 , P . 5 .

[370] د. عبد الفتاح عايد فايد ، التعويض التلقائي للاضرار بواسطة التأمين وصناديق الضمان ، دار الجامعة الجديدة ، الاسكندرية ، 2014 ، ص13 .

خامسا : الرجوع على المسؤول عن تعويض الضرر في حالة الوفاء بقيمة التعويض للمضرور :. اشارت القوانين المنظمة لحماية البيانات الشخصية الى انه يحق للشركة الرجوع على المتحكم او المعالج الضالع في عملية احداث الضرر للشخص المعني بالمبلغ الخاص بهم من المسؤولية عن الضرر ووفقا للشروط [371].

وبناء عليه يمكن القول بان تبني مبدأ حلول الموفي محل المضرور في الرجوع على فاعل الضرر و الذي تبنته التشريعات ، اشترطت لذلك ان يتم الامتثال لما نصت عليه الفقرة السابقة انفة الذكر .

وهذا التوجه يتوافق مع ما يراه جانب من فقه القانون المدني [372] ، من ان المسؤولية المدنية تبدو كنظام موجه نحو تعويض الاضرار ، هذا التعويض يتحقق عن طريق دفع مبلغ للمضرور يتطابق من حيث المبدأ مع الخسارة التي لحقت به والكسب الذي فاته ، هذه الصيغة تتجه من باب أولى نحو مفهوم اقتصادي بحت للتعويض .

ويؤكد جانب اخر من الفقه على ذات المعنى المتقدم من ان المستقر عليه في مجال المسؤولية المدنية ، ان الجبر الكامل للضرر الذي يلحق بالمضرور يحول دون أي افقار او اثراء لهذا الأخير ، وبالتالي فان الأموال التي يدفعها المسؤول تهدف الى إعادة الشخص المضرور الى الوضع الذي كان عليه قبل وقوع الضرر [373].

ومن المثير للاهتمام في هذا الصدد ان اعتماد التشريعات هنا على فكرة حلول الموفي محل المضرور تحقق اكثر من فائدة ، الأولى : ان يقع العبء النهائي للتعويض على عاتق الشخص المسؤول عن الضرر ، والثانية : منع اثراء المضرور من التعويض بعدم حصوله على تعويض يزيد عن الضرر الذي أصابه ، والثالثة : تخفيف التكلفة الاجتماعية للحصول على التعويض [374].

و يمكن القول بان دعوى الرجوع التي يمارسها الموفي ليست وسيلة لتحيد شخصية المسؤول ، بل هي وسيلة تهدف الى الرجوع على المسؤول بقيمة التعويض الذي اخذه على عاتقه الشخص الذي قام بالوفاء بقيمته للمضرور

---

[371] انظر نص المادة 82 /5 من اللائحة الاوربية العامة لحماية البيانات الشخصية لسنة 2016 .

[372] Suzanne Carval , Patrice Jourdain , Genevieve Viney ; Les effets de Ia responsabilite 4e edition , Editeur ; L.G.D.J, 2017,N 2,P.5.

[373] Linda Maizener , member du consell d,administration de I,Association des jeunes magistrats Tout Ie dommage , rien que Ie dommage ? Gaz , pal . 24 juill . 2018 , n GPL329s3 , p. 3

[374] Patrice Jourdain, Genevieve Viney : Traite de droit Civil , Les conditions de la responsabilite Dommage, fait generateur , regimes speciaux , causalite , 4e edition , Editeur:L.G.D.J , 2013 , P.88 .

المطلب الثاني

المسؤولية الجزائية

تتوزع الدراسة في اطار المسؤولية الجزائية عن انتهاك البيانات الشخصية في عدة محاور واهمها فيما يتعلق بجريمة الجمع غير المشروع للبيانات الشخصية ، وجريمة معالجة بيانات شخصية رغم اعتراض صاحب الشأن ، وجريمة الحفظ غير المشروع للبيانات الشخصية الحساسة ، وجريمة حفظ بيانات شخصية خارج الوقت المسموح به قانونا ، وجريمة الانحراف عن الغرض من المعالجة الالكترونية للبيانات الشخصية ، وأخيرا الاتجار غير المشروع وتداول البيانات الشخصية ، وسيقتصر موضوع دراسة هذه الجرائم على الركنين المادي والمعنوي دون التطرق الى موضوع هذه الجرائم جميعها ، الا وهو البيانات الشخصية والذي يعد الركن المشترك بينها ، حيث سنحيل في شأنه الى ما سبق ذكره سابقا ، وسنبين هذه الجرائم تباعا ، وحيث ان المشرع الأوربي لم ينظم العقوبات الجزائية وانما نص على انه تضع الدول الأعضاء القواعد المتعلقة بالعقوبات السارية على خرق هذه اللائحة على وجه الخصوص [375]، وعليه سنقوم بدراسة القانون الفرنسي كنموذج من قوانين الدول الاعضاء في الاتحاد الأوربي وكالاتي :

الفرع الأول

جريمة الجمع غير المشروع للبيانات الشخصية

تناول المشرع الفرنسي هذه الجريمة في المادة (226،18) من قانون العقوبات بانه " يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة الف يورو كل من جمع البيانات الشخصية بوسائل غير مشروعة او غير عادلة او احتيالية " [376]، في حين نص المشرع المصري عليها في قانون حماية البيانات الشخصية المصري على النحو الاتي " ويعاقب بغرامة لا تقل عن مائتي الف جنيه ولا تتجاوز مليوني جنيه كل من جمع بيانات شخصية دون توافر الشروط المنصوص عليها في المادة (3) من هذا القانون (الشروط الخاصة بجمع البيانات الشخصية) وسندرس هذه الجريمة من خلال بيان أركانها ومن ثم عقوباتها وكالاتي :

أولا : اركان الجريمة : يتضح من المادتين السابقتين ان الجريمة تتكون من ثلاثة اركان : موضوع هو البيانات الشخصية ، وركن مادي قوامه نشاط يتمثل بفعل جمع البيانات الشخصية بصورة غير مشروعة ، وركن معنوي صورته القصد الجنائي .

1- الركن المادي : نص كل من المشرعين الفرنسي والمصري على فعل واحد يقوم به الركن المادي لهذه الجريمة ، هو فعل تجميع البيانات الشخصية بوسيلة غير مشروعة او غير عادلة او احتيالية او بدون توافر الشروط المقررة قانونا ، اذ ان القوانين حددت هذه الشروط بالنص على ان الجمع يجب ان يكون لأغراض محددة وقانونية ولا يجوز جمعها لغير هذه الأغراض التي تم جمعها لاجلها [377]

.

وفيما يتعلق بالشروط فيرى الباحث انه لا يتعين الاخلال بها جميعها لاعتبار ان التجميع قد حدث بصورة غير مشروعة بل يكفي الاخلال باي شرط منها في معرض جمع البيانات ، لتقرير ان الاخلال بالشروط الخاصة بجمع البيانات الشخصية قد وقع بالفعل .

---

[375] انظر نص المادة (84/ 1) من اللائحة الاوربية (GDPR)

[376] نص المادة (226-18) من قانون العقوبات الفرنسي والمعدلة بموجب القانون رقم 801 لسنة 2004 .

[377] انظر نص المادة (b/1/5) من اللائحة الاوربية العامة لحماية البيانات الشخصية رقم 679 لسنة 2016 .

ويذهب جانب من الفقه الى ان ذلك يشمل الحصول على البيانات الشخصية بأي فعل او اجراء لا يحافظ على الحقوق الممنوحة للأشخاص المعنيين بحماية بياناتهم ، خاصة حق الاعتراض [378] .

وتتنوع المظاهر التي يتحقق فيها هذا الفعل الى صور كثيرة منها على سبيل المثال ، جمع البيانات في ظروف لا تسمح للمعنيين بها بممارسة حقهم بالمعارضة او الاعتراض [379] ، او الحصول على البيانات الشخصية دون سبب مشروع ، او عن طريق سرقة ملف او بالغش والتدليس ، ويرجع السبب في ذلك الى ان الالفاظ التي جاءت بها المادتان السابقتان هي من الاتساع بحيث يندرج تحتهما جميع الأفعال المذكورة وغيرها .

ومن التطبيقات القضائية التي تتصل بالجريمة " انه في عامي 2002-2003 ، أرسلت شركة رسائل بريد الكترونية غير مرغوب فيها الى افراد تم الحصول على عناوين بريدهم الالكتروني من المنطقة العامة لشبكة الانترنت ، وذلك في استخدام برنامج في البداية يخزن هذه المعلومات في ملف لاستخدامها لاحقا ، ثم في مرحلة ثانية باستخدام برنامج اخر يوجه الرسائل الاعلانية الى العناوين التي تم جمعها دون حفظها في ملف ، ولادانة الشركة ومديرها بالجريمة المنصوص عليها في المادة 226-18 من قانون العقوبات الفرنسي حكمت محكمة الاستئناف انها أي الشركة جمعت عناوين الكترونية والتي تشكل بيانات شخصية بطريقة غير عادلة من حيث انها قد استخدمت بشكل غير مرتبط بالغرض من نشرها ، حتى بدون تسجيلها في ملف ، وانما لارسال رسائل الكترونية الى أصحابها من ناحية ، فضلا عن انه من غير المنصف ان نجمع عناوين البريد الالكتروني الشخصية للأشخاص الطبيعيين من المنطقة العامة لشبكة الانترنت بدون علمهم ، فهذه العملية تعرقل حقهم في الاعتراض من ناحية أخرى [380] .

وفي الآونة الأخيرة ذهبت محكمة العدل في الاتحاد الأوربي الى ان مدير موقع الكتروني مجهز بزر "Like" في فيس بوك ، قد يكون مسؤولا بشكل مشترك مع فيس بوك عن جمع ونقل البيانات الشخصية لزوار الموقع الى فيس بوك [381].

2- الركن المعنوي : يتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي ، وهو مستفاد من طبيعة الأفعال التي تقوم بها الجريمة ، ويترتب على ذلك انها لا تقع بطريق الخطأ ، بمعنى انه لا يتصور وقوعها في صورة غير عمدية [382] .

والقصد الذي يتطلبه كل من المشرعين الفرنسي والمصري في هذه الجريمة هو القصد العام بعنصريه العلم والإرادة ، حيث يجب ان يعلم الجاني بالصفة الشخصية للبيانات ، وانه يقوم بتجميع هذه البيانات بوسيلة غير

---

[378] د. ماشاء الله عثمان محمد الزوي ، الحماية الجنائية لحرمة الحياة الخاصة في التشريع الليبي بالمقارنة مع التشريعين الفرنسي والمصري ، أطروحة دكتوراه مقدمة الى كلية الحقوق / جامعة القاهرة ، 2012، ص235 .

[379] Cass crim , 14 Mars 2006 , N de pourvoi ; 05-83423 , Bull . cirm . 2006 , N 69 , P . 267 , Disponible sur www .Iegifrance.gouv.fr, Ie : 4/12/2020.

[380] Cass crim , 14 Mars 2006 , N de pourvoi ; 05-83423 , Bull . cirm . 2006 , N 69 , P . 267 , Disponible sur www .Iegifrance.gouv.fr, Ie : 2/5/2020; D . 2007 . pan . 404 , obs . Gare ; AJ penal 2006 . 260, obs . Roussel .

[381] T .corr . Paris , 8 avril 2014 : D. actu . 17 avril 2014 , obs . Lavric , Disponible sur : www . dalloz . fr, Le : 02/5/2020 .

[382] أسماء حسن سيد محمد رويعي ، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية ، أطروحة دكتوراه مقدمة الى كلية الحقوق / جامعة القاهرة ، 2013، ص520 .

مشـروعة وغير عادلة ولم يراعي الشـروط المنصـوص عليها قانونا ، كما يجب ان تتجه ارادته الى ارتكاب هذا السلوك الاجرامي [383].

ومتى تحقق القصد الجنائي فلا عبرة بالبواعث التي دفعت الجاني الى ارتكاب فعله ، فيستوي ان يكون الباعث الاضرار المادي بالشخص المعني ، او الإساءة لسمعته ، او مجرد الفضول وحب الاستطلاع[384].

ثانيا : العقوبة : نص المشرع الفرنسي على عقوبتين لهذه الجريمة ، عقوبة اصلية وأخرى تكميلية ، والعقوبة الاصـــلية هي الحبس خمس ســنوات و الغرامة ثلاثمائة الف يورو ، وأيضـــا فرض عقوبة تكميلية تتمثل في حرمان الجاني من ممارسة الحقوق المدنية والاسرية ، كذلك حظر ممارسة النشاط المهني والاجتماعي الذي وقعت بسببه او بمناسبته الجريمة ، وحرمانه من حيازة او حمل السلاح المرخص لمدة أقصاها خمس سنوات ، وأخيرا لصق ونشر حكم الإدانة [385].

وهذا ويمكن ان تقوم المسـؤولية لجزائية للأشـخاص المعنوية عن الأفعال المنصـوص عليها في المادة 18-226 ، من قانون العقوبات الفرنسي ، وذلك اعمالا لحكم المادة 24-226 من القانون ذاته.

كما يمكن الحكم بمسح او حذف كل او بعض البيانات المعالجة والتي كانت محلا للجريمة بحضـور الشـخص المعني بالبيانات ووكلاء من اللجنة الوطنية للمعلوماتية والحريات [386].

ويعاقب المشرع المصري على الجريمة ذاتها بغرامة لا تقل عن مائتي الف جنيه ولا تتجاوز مليوني جنيه ، فضـلا عن ذلك تقضـي المحكمة بنشر حكم الإدانة في جريدتي واسعتي الانتشـار ، وعلى شبكات المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه ، كما أضـــاف القانون انه في حالة العود تضـــاعف العقوبات المذكورة بحديها الأقصى والادنى [387] .

واذا ارتكبت الجريمة من قبل احد العاملين لدى شـخص اعتباري ما ، وبأسم هذا الشـخص ولحسـابه ، يعاقب المســؤول عن الإدارة الفعلية للشـــخص الاعتبـاري بذات العقوبـات المقررة لها ، أي بذات عقوبات الفاعل الأصلي اذا ثبت علمه بها ، وكان اخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد اسهم في وقوع الجريمة ، إضافة لذلك يكون الشخص الاعتباري مسؤولا بالتضامن عن الوفاء بما يحكم به من تعويضات [388].

وأخيرا يشكل فعل جمع البيانات الشخصية بشكل غير مشروع جريمة مستمرة لا يحسب التقادم فيها الا من تاريخ انتهاء حالة الاستمرار [389].

الفرع الثاني

جريمة الحفظ غير المشروع للبيانات الشخصية الحساسة

---

[383] انظر نص المادة (226-18) من قانون العقوبات الفرنسـي والمعدلة بموجب القانون رقم 801 لسـنة 2004 ، وكذلك نص المادة (3) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

[384] د. أسماء حسن سيد محمد رويعي ، المصدر نفسه ، 577 .

[385] انظر الفقرات (1-2-3-4) من المادة (226-31) من قانون العقوبات الفرنسي ذي العدد 653 لسنة 1994 .

[386] انظر نص المادة 226- 23 من قانون العقوبات الفرنسي المعدلة بموجب الامر المرقم 1125 لسنة 2018 .

[387] انظر نص المادة 37 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[388] انظر نص المادة (47) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[389] د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، دراسة في القانون الفرنسي ، القسم الأول ، مصدر سابق ، ص433 .

تصنف بعض البيانات الشخصية على انها حساسة ، بحيث تهدد فيما اذا لو تم استخدامها او التعامل بها بطريقة خاطئة حريات الافراد ، وعلى هذا الأساس فقد جرم المشرع الفرنسي فعل التخزين او الحفظ غير المشروع لهذه البيانات [390] . في حين جرم المشرع المصري فعل جمع البيانات الشخصية الحساسة او تداولها او اتاحتها او معالجتها او تخزينها او افشائها او نقلها او حفظها بصورة غير مشروعة ، وعاقب مرتكبها بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة الف جنيه ولا تتجاوز خمسة ملاين جنيه او بإحدى هاتين العقوبتين [391] . وسنتناول هذه الجريمة من خلال بيان أركانها ومن ثم عقوبتها وكالاتي :

أولا : اركان الجريمة : هذه الجريمة كسابقتها تتطلب توافر ثلاث اركان ، موضوع الجريمة وهو البيانات الشخصية التي تتصف بطبيعة خاصة وحساسة ، وركن مادي ومعنوي ، وسنكتفي ببيان الثاني والثالث دون الأول الذي تم بيانه في الفصل الأول وكالاتي :

1- الركن المادي : يقوم هذا الركن على عنصرين : السلوك الاجرامي وعدم رضا الشخص المعني بمعالجة البيانات او القيام بلك في غير الأحوال المصرح بها قانونا :

أ- السلوك الاجرامي : حدد المشرع الفرنسي صورتين لهذا السلوك هما : التسجيل او الحفظ في ذاكرة معلوماتية ، في حين حدد المشرع المصري صور هذا السلوك بطريقة أوسع ، فاضاف الى العنصرين السابقين الصور الاتية : الجمع او التداول او الاتاحة او المعالجة او النقل او الافشاء .

ب- عدم رضا الشخص المعني (صاحب البيانات) بمعالجة البيانات او القيام بذلك في غير الأحوال المصرح بها قانونا : اشترط كل من المشرعين الفرنسي والمصري ان تتم معالجة البيانات الشخصية الحساسة بإحدى صورها سالفة الذكر دون رضاء الزبون ، مما يعني اذا توفر الرضاء لا محل لقيام الجريمة ، الا انه يشترط في الرضاء هنا ان يكون صريحا وفقا للتشريع الفرنسي [392] . وعلى العكس من ذلك بالنسبة للتشريع المصري في المادة (41) من قانون حماية البيانات الشخصية فانه لم يشترط صراحة ان تكون الموافقة صريحة ، و يستوي لديه ان تكون هذه الموافقة صريحة ام ضمنية . كما انه لا محل للجريمة أيضا اذا تم التجميع او التخزين لهذه البيانات او اتاحتها او معالجتها او تداولها او نقلها او افشائها في الأحوال التي يسمح بها القانون ، ونحيل في هذا الشأن لما تم ذكره سابقا .

وعلى الصعيد القضائي فقد قضي في فرنسا بقيام هذه الجريمة في حق شخص قام بتجميع او تخزين البيانات المتعلقة بعدد حالات الزواج بين الفرنسيين وغيرهم من الجنسيات الأخرى ، والاراء السياسية الخاصة بهم في ذاكرة معلوماتية بدون موافقة الأشخاص المعنيين[393].

---

[390] نصت المادة (226-19) من قانون العقوبات الفرنسي المعدلة بالمرسوم المرقم 1125 لسنة 2018 على انه " يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة الف يورو كل من يسجل او يحفظ في ذاكرة معلوماتية بدون موافقة صريحة من الشخص المعني ، البيانات الشخصية التي تكشف بصورة مباشرة او غير مباشرة عن الأصول العنصرية او العرقية او الآراء السياسية او الفلسفية او الدينية او الانتماءات النقابية للأشخاص ، او التي تتعلق بصحة القانون ، ويعاقب بالعقوبة ذاتها كل من يسجل او يحفظ في ذاكرة معلوماتية البيانات الشخصية المتعلقة بالجرائم او احكام الإدانة او التدابير الاحترازية ، بخلاف الحالات التي ينص عليها القانون ، تنطبق احكام هذه المادة على المعالجة غير الالكترونية للبيانات الشخصية التي لايقتصر تنفيذها على ممارسة الأنشطة الشخصية المحضة ".

[391] انظر نص المادة (41) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[392] انظر نص المادة (226-19) من قانون العقوبات الفرنسي المعدلة بالمرسوم المرقم 1125 لسنة 2018

[393] Cass . Crim , 16 mars 2004 , N de pourvoi : 04 – 80048 , Disponible sur www . Iegifrance . gouv . fr, le : 7/9/2021 .

وهذه الجريمة كما السابقة تعد جريمة مستمرة طالما ان النشاط الجرمي يتمثل في التسجيل او الحفظ في ذاكرة النظام للبيانات الشخصية الحساسة ، وتنتهي الجريمة بانتهاء حالة الاستمرار ، و لا تبدأ مدة التقادم في الاحتساب الا من تاريخ تخلي الجاني عن هذه البيانات ، أي من تاريخ انتهاء حالة الاستمرار .

2- الركن المعنوي يتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام بعنصريه العلم والإرادة ، وهذا مستفاد من طبيعة الأفعال التي تقوم عليها الجريمة ، فيجب ان يعلم الجاني بالإضافة الى الطبيعة الشخصية للبيانات ، بالصفة الخاصة لهذه البيانات والتي تجعلها تدخل في عداد الفئات الحساسة من البيانات والتي يحظر القانون معالجتها من حيث المبدأ [394] . وكما يجب ان يعلم الجاني بنشاط المعالجة الالكترونية وبعدم مشروعية هذه المعالجة لعدم التقيد باحكام القانون فيما يتعلق بهذا الشأن ، وكذلك يجب ان تتجه إرادة الجاني الى معالجة هذه البيانات مخالفا بذلك الحظر المقرر قانونا لمعالجتها ، ولا عبرة بالبواعث التي دفعت الجاني الى ارتكاب فعله [395] .

ثانيا : العقوبة : نلاحظ من المادة (226-19) من قانون العقوبات الفرنسي ان عقوبة الجريمة الواردة فيها هي ذات عقوبة الجريمة الواردة في المادة (226-18) من القانون ذاته ، مما يعني فهي تخضع لما سلف تفصيله في شأن هذه العقوبة الأخيرة من احكام .

وكذلك تعاقب المادة (41) من قانون حماية البيانات الشخصية المصري بالحبس مدة لاتقل عن ثلاثة شهور وبغرامة لاتقل عن خمسمائة الف جنيه ولاتزيد عن عن خمسة ملاين جنيه ، او بإحدى هاتين العقوبتين .

كما نجد من خلال استقراء المادتين (47-48) من قانون حماية البيانات الشخصية المصري ان الجريمة محل البحث تخضع للاحكام الواردة في هاتين المادتين ، والتي تتعلق بالشخص الاعتباري ، ونشر الحكم والعود ، والتي سبق بيانها .

الفرع الثالث

جريمة حفظ بيانات شخصية خارج الوقت المسموح به قانونا

نص المشرع الفرنسي على هذه الجريمة وفرض عليها عقوبة بقوله يعاقب بالحبس خمس سنوات او الغرامة ثلاثمائة الف يورو كل من يقوم بالاحتفاظ ببيانات شخصية لمدة اكثر من المدة المنصوص عليها في القانون او اللائحة ، بناء على الترخيص (الاذن) او الاشعار او الاخطار (الإعلان) المسبق الموجه للجنة الوطنية للمعلوماتية والحريات ، مالم يتم حفظها لأغراض تاريخية او إحصائية او علمية على النحو المنصوص عليه في القانون [396] . في حين أوردها المشرع المصري في عداد الجرائم المنصوص عليها في المادة (38) من قانون حماية البيانات الشخصية . وسندرس هذه الجريمة من خلال بيان أركانها ومن ثم عقوبتها وكالاتي .

أولا : اركان الجريمة : تقوم هذه الجريمة على أركان ثلاثة : موضوع، وهو البيانات الشخصية. وركن مادي قوامه نشاط يتمثل بفعل الاحتفاظ غير المشروع لهذه البيانات. وركن معنوي يتخذ صورة القصد الجنائي. ويضاف إلى ذلك أن المشرع المصري تطلب شرطاً أولياً سابقاً لقيام هذه الجريمة، وهو أن يكون مرتكب الجريمة متحكماً أو معالجاً، بالمعنى المقصود به في المادة (1) من قانون حماية البيانات الشخصية[397].

---

[394] د. ماشاء الله عثمان محمد الزوي ، مصدر سابق ، ص 239 .

[395] د. عمار عباس الحسيني ، جرائم الحاسوب والانترنت ، الجرائم المعلوماتية ، منشورات زين الحقوقية ، ط1 ، بيروت ، لبنان ، 2017 ، ص 242 .

[396] انظر نص المادة (226-20) من قانون العقوبات الفرنسي المعدلة بموجب الامر رقم 801 لسنة 2004 .

[397] يقصد بالمتحكم طبقاً للمادة (1) من قانون حماية البيانات الشخصية المصري بأنه : "أي شخص طبيعي أو اعتباري، يكون له-بحكم أو طبيعة عمله-الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو

1- الركن المادي : يتحقق هذا الركن-بحسب التشريع الفرنسي-بقيام الشركة بحفظ البيانات الشخصية لمدة أطول من المدة المسموح بها قانوناً ، ما لم يكن ذلك الحفظ للبيانات لاغراض تاريخية أو إحصائية أو علمية وطبقاً للشروط أو بمعالجة تلك البيانات المحفوظة لما بعد المدة المسموح بها قانوناً لاغراض أخرى غير تلك المقصودة (أي المعالجة لاغراض غير الاغراض التاريخية أو الاحصائية أو العلمية للبيانات الشخصية المحتفظ بها بعد الفترة المشار إليها [398].

أما المشرع المصري فقد فرض على عاتق المتحكم والمعالج الالتزام بمدد زمنية للاحتفاظ بالبيانات الشخصية ومعالجتها [399]، وعلى ذلك تقع الجريمة متى خالف المتحكم أو المعالج الالتزام المذكور بقيامه بحفظ البيانات الشخصية لمدة أطول من المدة المسموح بها قانوناً .

ومن الجدير بالذكر ان وقوع هذه الجريمة يفترض بدايةً أن تكون عملية المعالجة والحفظ للبيانات الشخصية قد تمت وفقاً لاحكام القانون، ومن ثم تم حفظ البيانات لمدة تجاوز المدة المرخص بها أو المطلوبة للحفظ .

وتطبيقا لذلك، فقد قضي "أنه مذنب بالاحتفاظ بمعلومات اسمية دون موافقة CNIL ،بعد الفترة المنصوص عليها في طلب الاخطار أو الاعلان المسبق، المدير الفعلي لشركة احتفظت بشكل غير قانوني بشفرات البطاقات الائتمانية للزبائن على الرغم من أنه لا يمكن استخدام هذه البيانات المصرفية، ولا يجوز الاحتفاظ بها إلا في حالة الضرورة الشديدة، ولمدة معاملة معينة، ولكن لا يجوز تخزينها تحت أي ظرف من الظروف"[400] .

2- الركن المعنوي : جريمة حفظ البيانات خارج الوقت المسموح به قانونا ، جريمة عمدية، يتمثل فيها الركن المعنوي في صورة القصد الجنائي بعنصريه ّ العلم والارادة، فيجب أن يعلم الجاني بمختلف عناصرها ؛ وتطبيقاً لذلك لا بد أن يدرك الجاني الطبيعة الشخصية للبيانات، وأنه يقوم بفعل الاحتفاظ بهذه البيانات لمدة أطول من المدة المسموح بها قانوناً، أو بمعالجة البيانات المحفوظة - بحسب التشريع الفرنسي لما بعد المدة المسموح بها قانوناً لاغراض أخرى غير تلك المقصودة، بخلاف ما ينص عليه القانون. وكما يجب أن تتجه إرادة الجاني إلى تحقيق ذلك مخالفاً الحظر الذي قرره القانون [401].

واستنادا اما سبق ذكره فان هذه الجريمة لا تقع عن طريق الخطأ. ولا عبرة للبواعث التي دفعت الفاعل إلى ارتكاب جريمته، فسواء أن يكون باعثه إلى ذلك هو ابتزاز المجني عليه للحصول على المال أم التشهير به أم الحصول على مغنم معنوي [402].

معالجتها والتحكم فيها طبق للغرض المحدد أو نشاطه". في حين عَرفت المادة ذاتها المعالج بأنه : "أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه، أو لصالح المتحكم بالاتفاق معه ووفقاً لتعليماته".

[398] د. ما شاء الله عثمان الزوي، الحماية الجنائية للبيانات الشخصية الالكترونية في القانون الليبي والمقارن، مجلة العلوم الشرعية والقانونية، كلية القانون بالخمس، جامعة المرقب، العدد الأول ، 2018 ،ص 186 .

[399] انظر نص البندين (9-3) من المادتين (4-5) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[400] (Cass. Crim., 3 mars 2015, N° de pourvoi : 13-88079, Disponible sur: www.legifrance.gouv.fr, Le : 02/05/2021.

[401] د . شول بن شهرة، د/ ماجدة مدوخ، حماية الخصوصية في المعاملات المالية الاسلامية، (بيانات عملاء العمليات المصرفية الالكترونية نموذجاً) ، بحث منشور في مجلة معهد العلوم الاقتصادية والتجارية والتسيير في الجزائر ، 2011، ص 11.

[402] د. سعاد علي محمد الفقيه، الحماية الجنائية للحياة الخاصة في القانون الليبي، المرجع السابق، ص 482.

ثانيا : العقوبة : نلاحظ ان المشـــرع الفرنســـي نص على عقوبة الجريمة الواردة هنا بذات عقوبة الجريمة الواردة في المادة 18-226 من القانون ذاته ، وبالتالي فهي تخضـع لما سـلف تفصـيله في شـأن هذه العقوبة الاخيرة من أحكام .

وتعاقب المادة (38) من قانون حماية البيانات الشـخصـية المصـري على ذات الجريمة بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه. كما نجد من خلال اسـتقراء المادتين (47 ،48) من قانون حماية البيانات الشخصية المصري أن الجريمة محل البحث تخضع للاحكام الواردة في هاتين المادتين، والتي تتعلق بالشخص الاعتباري، ونشر الحكم وحالة العود ؛ لذلك سوف نحيل في شأنها إلى ما سبق أن أوضحناه لدى دراستنا لجريمة الجمع غير المشروع للبيانات الشخصية المنصوص عليها في الفقرة الثانية من المادة (37) من القانون ذاته .

الفرع الرابع

جريمة الانحراف عن الغرض من المعاجلة الالكترونية للبيانات الشخصية

يعَّد مبدأ الغاية أو الغرض من المبادئ الاساسية في القوانين الناظمة لحماية البيانات ، ويتطلب هذا المبدأ الا يتَّم تجميع البيانات او معالجتها الا لهدف أو غرض محدد وواضـــح ومشـــروعٍ [403]، وعلاوة على ذلك فقد فرض المشـرع المصـري التزاماً على عاتق كل من المتحكم والمعالج بالتأكد من انطباق الغرض المحدد من جمع البيانـات الشـــخصـــيـة لاغراض معـالجتها، وعدم تجاوز هذا الغرض، وذلك عملا بالبندين (3،4) من المادتين (4،5) على التوالي من قانون حماية البيانات الشـخصـية المصـري، و لا يمكن طلب أو جمع بيانات شخصية غير مرتبطة بهذا الغرض ، أو الخروج عنه بمناسبة معالجة البيانات المقصودة به [404]؛ وعلى هذا المنوال جَّرم المشـــرع الفرنســـي فعل الانحراف عن الغرض أو الغاية المحددة للمعالجة الالكترونية للبيانات الشـخصـية ، بقوله : "يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من حاز بيانات شـخصـية بمناسـبة قيامه بتسـجيلها أو تصـنيفها أو نقلها أو معالجتها تحت أي شـكل، إذا غير من الوجهة النهائية المقَّررة لهذه البيانات وفقاً للقانون أو للقرار الصادر في شأنها أو في الاخطار المسبق على القيام بالمعالجة" [405].

في حين أورد المشـرع المصـري هذه الجريمة في عداد الجرائم المنصـوص عليها في المادة (38) من قانون حماية البيانات الشـخصـية المصـريُ على النحو الاتي: " يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، كل متحكم أو معالج لم يلتزم بواجباته المنصـــوص عليها في المواد (4،5،7) من هذا القانون". وسنتناول هذه الجريمة من خلال بيان أركانها ومن ثم عقوبتها وعلى النحو الاتي :

أولا : أركان الجريمة : تقوم هذه الجريمة على ثلاثة أركان : موضوع، وهو البيانات الشخصية، وركن مادي يتمثل في قيام الشركة بإساءة استخدام أو استغلال هذه البيانات، و ركن معنوي يتخذ صورة القصد الجنائي و

---

[403] انظر في ذلك المادة (1/3) من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

[404] د.احمد عرف احمد يوسـف ، الاعتداء على الحياة الخاصـة في مواقع التواصـل الاجتماعي ، بحث منشـور في مؤتمر الضوابط القانونية والاخلاقية للاعلام ، كلية الحقوق – جامعة عين شمس ، 2018 ، ص 264 .

[405] Article 226-21 : "Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

يضـاف الى ذلك ان كلا المشـرعين الفرنسـي و المصـري قد تطلب شـرطاً أولياً سـابقاً إلى ذلك لقيام هذه الجريمة، حيث يتمثل هذا الشرط - بحسب التشريع الفرنسي - في ضرورة أن يكون مرتكب الجريمة ممن حازوا بيانات شخصية بمناسبة تسجيلها أو تصنيفها أو نقلها أو لعالجها إلكترونياً تحت أي شكل ، كالمسؤول عن المعالجة traitement du responsable؛ والمتعاقد معه من الباطنsous-traitant ؛ والمتلقي (المرسل إليه destinataire)؛ وغيرهم. و نحيل-منعاً للتكرار-في شأن تعريف كل واحد منهم إلى ما سلف بيانه . في حين أشار المشرع المصري إليه بضرورة أن يكون مرتكب الجريمة متحكماً أو معالجاً، بالمعنى المقصود به في المادة (1) من قانون حماية البيانات الشخصية.

1- الركن المادي : يتمثل السـلوك الاجرامي هنا في فعلٍ واحدٍ وهو الانحراف عن الغاية من المعالجة الالكترونية للبيانات الشـخصـية، ويعُّد الركن المادي متحققاً بمجرد اقتراف هذا الفعل، ويسـتوي أن يحدث ذلك في مرحلة تسجيل البيانات أو تصنيفها أو نقلها أو في أي مرحلة من مراحل التعامل معها [406]. والغاية هي موضوع المعالجة الالكترونية، أي الغرض المتوخى من معالجة البيانات الشخصية وهي المبرر الوحيد لمعالجة البيانات الشـخصـية إلكترونياً [407] . وتفترض هذه الجريمة بدايةً الحصول على البيانات بصورة مشروعة، و من ثم ضرورة تحديد الغاية من معالجة هذه البيانات إلكترونياً بشكل دقيق وواضح، ولكن الشركة تنحرف في النهاية عن هذه الغاية[408] .
2- الركن المعنوي : جريمة الانحراف عن الغرض أو الغاية من المعالجة إن الالكترونية للبيانات الشخصية جريمة عمدية يتمثل فيها الركن المعنوي في صورة القصد الجنائي العام بعنصريه العلم والارادة، فيجب أن يعلم الجاني بموضـوع الحق المعتدى عليه من حيث أنه بيانات ذات طابع شخصي، وبالغرض المتوخى من معالجة هذه البيانات إلكترونياً، كما يتعين أن يعلم بأن من شأن فعله الانحراف أو الخروج عن هذا الغرض، وأن تتجه إرادته إلى تحقيق ذلك [409].

وتطبيقاً لذلك فإنه إذا استغل شخص بيانات خاصة بآخر، في الكشف عن مركزه المالي أو حالته الصحية أو في الاسـتدلال عليه أو في الكشـف عن مصـادر ثروته ، من خلال قيامه بالانحراف عن الغاية من المعالجة الالكترونية للبيانات الشخصية الخاصة بصاحب البيانات ؛اذ يعد الركن المعنوي لهذه الجريمة متحققاً بحقه، ويعد حينها مرتكباً لهذه الجريمة [410].

وتسـتوي البواعث التي دفعت الجاني إلى اقتراف فعله، فسـواء أن يدفعه إليه باعث ابتزاز المجني عليه أو تحقيق منفعة للجاني أو دفع ضرر عنه أو تحقيق مصلحة للغير.

ثانيا : العقوبة : نلاحظ من المادة 21-226 من قانون العقوبات الفرنسـي أن عقوبة الجريمة الواردة فيها هي ذات عقوبة الجريمة الواردة في المادة 18-226 من القانون ذاته، وعليه فهي تخضـع لما سـلف تفصـيله في شأن هذه العقوبة الاخيرة من أحكام . كما نجد-بحسب التشريع المصري-أن عقوبة هذه الجريمة تتساوى مع عقوبة جريمة حفظ بيانات شـخصـية خارج الوقت المسـموح به قانوناً ؛ لان هاتين الجريمتين تندرجان في نطاق المادة (38) من قانون حماية البيانات الشخصية المصري ذات العقوبة الواحدة ؛ لذلك نحيل في شأن أحكام العقوبة إلى ما سبق بيانه لدى دراستنا لعقوبة هذه الجريمة الاخيرة منعاً للتكرار .

---

[406] د. غنام محمد غنام، الحماية الادارية والجنائية للافراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر، بحث منشور في مجلة الامن والقانون والتي تصدر عن كلية الشرطة في دبي ، العدد الثاني ، 2003، ص 102.

[407] د. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، مصدر سابق، ص155.

[408] د. سعاد علي محمد الفقيه، الحماية الجنائية للحياة الخاصة في القانون الليبي، مصدر سابق، ص 484.

[409] د . عمار عباس الحسيني، جرائم الحاسوب والانترنت (الجرائم المعلوماتية) ، مصدر سابق، ص 244.

[410] د . علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، مصدر سابق، ص 362 .

المبحث الثاني

القيود المترتبة على قيام المسؤولية

تقوم المسـؤولية بشـقيها المدنية والجزائية اذا لم تراعي الشـركة الالية القانونية اللازمة للتعامل مع البيانات الشخصية لزبائنها ، ولا يمكن ان تعفى هذه الشركة من المسؤولية الا اذا كان هناك قيد يمنع قيامها كما لو كان الامر يتعلق بالامن القومي وتمويل الإرهاب ، او كانت طبيعة المعاملة تقتضـي الكشـف عن بيانات الزبائن ، كما في حالة التحويل المالي الالكتروني ، وهو ما سنتناوله في هذا المبحث من خلال المطلبين الاتيين :

المطلب الأول

القيود المفروضة لمنع تمويل الإرهاب

شـكلت أحداث الحادي عشـر من سـبتمبر من عام 2001 نقطة تحول مهمة في مسـيرة العالم مع الظاهرة الارهابية، حيث برزت جريمة تمويل الارهاب مع ظهور تنظيمات إرهابية عديدة . وبالنظر إلى أهمية مكافحة هذا النوع من الاجرام، الذي يوفر منابع يغذي الجرائم الارهابية، فان المؤسسات المالية والمنظمات الدولية تتكاتف في مكافحة جريمة تمويل الارهاب، وذلك من أجل تجفيف منابع التمويل، ومن ثم الحد من الجرائم الارهابية، والتي تستند على الاموال التي ترصد لها، في حالة وضع آليات تحد من وصولها والوقوع في أيدي الارهابيين .

وبدأت العديد من الجهات المصـرفية في تتبع والتحفظ على الاصـول والودائع الخاصـة ببعض المنظمات والهيئات المتصلة بالجماعات الارهابية أو تلك التي تقوم بتمويل العمليات الارهابية. كما أن غالبية التشريعات في العالم لم تجرم جريمة تمويل الارهاب إلا في نهاية التسعينيات من القرن الماضي، حيث أصبحت جريمة قائمة بذاتها، وسنت غالبية الدول قوانين ضد الارهاب للتغلب على هذه الظاهرة على المستوى الوطني قبل تجريم تمويل الارهاب .

ولقد بذلت جهود دولية لمكافحة تمويل الارهاب، أهمها تلك الجهود التي قامت بها المجموعة الدولية للعمل المالي وتوصـياتها (FATF) [411]، وتتمثل مكافحة تمويل الارهاب الجبهة الاسـاسـية في الحرب على

---

[411] يطلق هذا الاسم على المجموعة الدولية للعمل المالي (Force Task Action Finance) المعنية بالاجراءات المالية على المستوى الدولي ، حيث تلعب دورا مهما في مكافحة غسيل الاموال وتمويل الارهاب؛ فتبذل جهودا في رفع مستوى تبني إجراءات مكافحة تلك العمليات، وقد تم تشكيل هذه المجموعة أثناء اجتماع الدول الصناعية السبع الكبرى (G7) باريس سنة 1989 وهي ايطاليا، وفرنسا ، وأمريكا، وبريطانيا، وكندا، واليابان، وألمانيا.

الارهاب، وذلك لان المال يعتبر المحرك الرئيسي للجماعات الارهابية، والمكون الاساسي لها، فمن خلال تمويل هذه الجماعات تتمكن من تجنيد الارهابيين، وتعدهم وتدربهم بواسطته، وتوفر به المستلزمات الضرورية، وأدوات التنفيذ من أسلحة، ومتفجرات، وآلات، وهكذا، فالتمويل هو أساس نجاح العمليات الارهابية، والعنصر الفاعل في تحقيق أهدافها. وعليه فان منع تمويل الارهاب وقمعه يتطلب تعاونا دوليا شاملا متسما بحسن النية لمحاصرة وتجفيف مصادر تمويل الارهاب، وتجريم المساعدة على تمويل الارهاب ، وكذلك ضرورة التعاون وتبادل المعلومات حول الانشطة المشبوهة، وإجراء رقابة فاعلة على الحسابات المصرفية وحركات الاموال بين الدول ، خصوصا على شبكة الانترنت وهو ما يعنينا في هذا البحث ، لذلك سنحاول ان نبين في هذا المطلب تحديد مفهوم تمويل الإرهاب ، وكذلك بيان الية منعه وكالاتي :

الفرع الأول

مفهوم تمويل الإرهاب

شغل موضوع الارهاب وتمويله حيزا كبيرا من اهتمام فقهاء القانون ، لما ينتج عن هذه الجرائم من آثار سلبية خطيرة، تهدد أمن المجتمع بشكل خاص والدولة بشكل عام، من خلال تدمير الممتلكات، وانتهاك الحرمات، وتدنيس للمقدسات، وقتل وخطف للمدنيين الامنين وتهديد لحياتهم واستقرارهم [412].

وإذا كان تمويل الارهاب يشكل عنصرا أساسيا وجوهريا لابد منه لتنفيذ واستمرار العمليات الارهابية، لان المال يعتبر عصب الجماعات الارهابية، والمكون الاساسي لها ، فمن خلال تمويل هذه الجماعات تتمكن من تجنيد الارهابيين، وتعدهم وتدربهم بواسطته، وتوفر به المستلزمات الضرورية، وأدوات التنفيذ من أسلحة، ومتفجرات، وآلات، وهكذا، فالتمويل هو أساس نجاح العمليات الارهابية، والعنصر الفاعل في تحقيق أهدافها. لذلك فان تحديد مفهوم التمويل ومصادره يضحى أمر بالغ الأهمية [413] .

كما أن مصطلح تمويل الارهاب ظهر حديثا ضمن مصطلحات القانون ، فالتجريم والعقاب المفروض كانا ينصبان على مكافحة الارهاب فقط ، ولم يتم الالتفات إلى تجريم تمويل الجماعات الارهابية وتجميد أموالها بشكل واضح ، كوسيلة لتجفيف منابع الارهاب، إلا عام 1999 ، بعد صدور الاتفاقية الدولية لقمع تمويل الإرهاب [414].

ويمكن القول بأن تمويل الارهاب هو نوع من المساهمة الجنائية أو الاشتراك بالمساعدة في الاعمال الإرهابية ، وإذا أخذنا بذلك فهو مجرم بتجريم العمل الارهابي وتابع له ، ولكن التمويل له أبعاد متعددة تتعدى نطاق المساعدة بالنظر إلى تعدد مصادره وتشعبها واضطلاع دول - في بعض الاحيان - به، ومن ثم اهتمت التشريعات الوطنية والاتفاقيات الدولية - والفقهاء من قبل م بوضع مفهوم محدد للتمويل ، ومن هذا المنطلق سنتناول تعريف تمويل الارهاب وبيان مصادره وكالاتي :

---

[412] د. منتصر سعيد حمود، الارهاب الدولي، جوانبه القانونية، ووسائل مكافحته في القانون الدولي العام والفقه الإسلامي ، ط1، دار الفكر الجامعي، الإسكندرية ، 2008 ، ص11.

[413] د. أسامة عبد المنعم علي إبراهيم، حصر ومكافحة غسيل الاموال ومكافحة تمويل الارهاب والنقل غير المشروع للاموال عبر الحدود في التشريعات العربية ، ط1، المركز القومي للاصدارات القانونية ، 2009 ، ص114.

[414] د. محمد السيد عرفة، الاتفاقية الدولية لقمع تمويل الارهاب ومدى فاعليتها في مكافحته، دراسة تأصيلية تحليلية مقارنة، جامعة نايف العربية للعلوم الامنية، الرياض، 2013 ، ص 9.

أولا : تعريف تمويل الإرهاب : يمكن تناول تعريف تمويل[415] الإرهاب في الفقه وبعض التشريعات الوطنية والاتفاقيات الدولية والإقليمية، وذلك على النحو التالي:

1- تعريف تمويل الإرهاب في الفقه : لا يوجد لدى الغالبية العظمى من الشراح والباحثين والفقهاء تعريفٌ محدد لمصطلح "تمويل الإرهاب" K ولكن يمكن تعريفه على أنّه: " بذل المال أو ما تقوم مقامه من إمكانات أو موارد أو جهود أو المشاركة المباشرة أو غير المباشرة في توفير الأموال النقدية أو العينية، سواء بالعطاء والتبرع أو الجمع بطريقة مشروعة أو غير مشروعة أو تغطية، أو تسهيل أو تمويل أو استثمار أو نقل أو تحويل أو توصيل هذه الأموال بهدف تمويل إرهابيين أو منظّمات أو عمليات إرهابية. [416]،

وذهب البعض الى أنّه يقصد بتمويل الإرهاب: (أي دعم مالي – في مختلف صوره - يقدم إلى الأفراد أو المنظّمات التي تدعم الإرهاب أو تقوم بالتخطيط لعمليات إرهابية، وقد يأتي هذا التمويل من مصادر مشروعة كالجمعيات الخيرية مثلاً، أو مصادر أخرى غير مشروعة مثل تجارة البضائع التالفة أو تجارة المخدرات) [417].

2- تعريف تمويل الإرهاب في التشريع: لا يوجد اتفاق دولي على تعريف موحدة لمصطلح تمويل الارهاب Financing Terrorism ، " ولعل ذلك نابع من عدم اتفاقها على تعريف مصطلح الإرهاب نفسه ، لذا تعددت التعريفات التي سيقت لمصطلح تمويل الإرهاب في التشريعات المقارنة ، فقد عرفه المشرع العراقي (كل فعل يرتكبه أي شخص يقوم بأية وسيلة كانت مباشرة او غير مباشرة ، بارادته بتوفيرالاموال او جمعها او الشروع في ذلك ، من مصدر شرعي او غير شرعي ، بقصد استخدامها مع علمه بان تلك الأموال ستستخدم كليا او جزئيا في تنفيذ عمل إرهابي او من إرهابي او منظمة إرهابية ، سواء وقعت الجريمة ام لم تقع وبصرف النظر عن الدولة التي يقع فيها هذا الفعل ، او يتواجد فيها الإرهابي او المنظمة الإرهابية)[418]، اما في فرنسا فقد جائت الفقرة (2-2)من المادة 421 من قانون العقوبات الفرنسي، المعدل بالقانون 2001-1062 المؤرخ 15 تشرين الثاني 2001 معرفة لجريمة تمويل الارهاب بالعبارات التالية : " ويشكل أيضا عملا من أعمال الارهاب تمويل منظمة إرهابية عن طريق توفير أو جمع أو إدارة أموال أو أوراق مالية أو ممتلكات من أي نوع كان أو تقديم المشورة من أجل هذا الغرض بقصد استخدام تلك الاموال أو الاوراق المالية أو الممتلكات أو مع العلم بأن القصد منها أن تستخدم كليا أو جزئيا من أجل ارتكاب أي من الاعمال الارهابية المذكورة في هذا الفصل بصرف النظر عن حدوث أو عدم حدوث ذلك العمل فعلا " ، وتؤكد فرنسا على أهمية منع حصول الارهابيين على أموال التبرعات الخيرية، بل حتى مجرد تقديم المشورة يدخل في نطاق تمويل الإرهاب حتى وان لم يحدث العمل الإرهابي [419].

---

[415] التمويل لغة يعني إعطاء المال وتقديمه، والتمويل مشتقٌ من المال، والجمع أموال، وقد وردت هذه الكلمة في القرآن الكريم في عدة مواضع، فيقول االله سبحانه وتعالى: ﴿وآتَى الْمالَ علَىٰ حبهِ ذَوِي الْقُربىٰ والْيتَامىٰ والْمساكِين ﴾ الآية (١٧٧) من سورة البقرة، وقوله تعالى أيضا: ﴿والَّذِين فِي أَموالِهِم حقٌّ معلُوم﴾ الآية (٢٤) من سورة المعارج. للمزيد من التفاصيل عن معنى التمويل لغة انظر: ابن منظور، لسان العرب، ج (٤) دار صادر للطباعة والنشر، دار بيروت للطباعة والنشر، بيروت، ١٩٥٦م، ص٦٣٦ ،الفيروز آبادي، القاموس المحيط، ج (٤) دار العلم للجميع، بيروت، ص ٥٢ .

[416] سالم علي الظنحاني، الإطار القانوني لمكافحة تمويل الإرهاب «دراسة قانونية سياسية»، بحث منشور في مجلة الشرق الأوسط، والتي تصدر عن مركز بحوث الشرق الأوسط بجامعة عين شمس، مصر، عدد (33) سبتمبر ٢٠١٣م، ص ٥٩٤.

[417] د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠٠٩م، ص٢١ وما بعدها.

[418] المادة (10/1) من قانون مكافحة غسيل الأموال وتمويل الإرهاب رقم 39 لسنة 2015 .

[419] خالد جمال حامد عبد الشافي، المواجهة التشريعية لظاهرة الارهاب، دراسة مقارنة، اطروحة دكتوراه مقدمة الى كلية الحقوق جامعة عين شمس ،2015، ص 50 ،51 .

بالمقابل فان المشرع الأمريكي يعرف في الفصل الخاص بتحديد المنظمات الارهابية الاجنبية الواقع في نطاق القسم (219) من تشريع الهجرة والجنسية الامريكية وتعديلاته، التي أدخلت بموجب أحكام تشريع مكافحة الارهاب وعقوبة الاعدام الفعالة الصادر في عام1996 تمويل الارهاب بأنه: قيام أي شخص موجود في الولايات المتحدة أو خاضع لولايتها القضائية بتوفير دعم أو موارد مادية إلى إحدى المنظمات الارهابية الاجنبية المحددة، حال علمه بذلك .

كما نص على أنه لا يجوز قبول دخول ممثلي أو أعضاء المنظمات الارهابية الاجنبية المحددة إلى أراضي الولايات المتحدة - إذا لم يكونوا مواطنين أمريكيين - كما يجوز إبعادهم من الولايات المتحدة في حالات محددة. ويجب على أية مؤسسة مالية تابعة للولايات المتحدة حال علمها بأنها تحوز أو تسيطر على أموال تعود بالنفع على إحدى المنظمات أن تخطر الجهات المختصة .

وفي 26 أكتوبر 2001 أصدرت الولايات المتحدة الامريكية المرسوم الوطني Patriot Act لمكافحة الارهاب، والذي فرض الجزء (351) منه على المؤسسات المالية أن تراقب كل النشاطات المالية وأن تبلغ عن أية نشاطات مريبة دون إمكانية ملاحقتها قضائيا ودون إبلاغ الشخص المعني لمواجهة عمليات تمويل الإرهاب[420].

من خلال استقراء ما ورد من تعريف للارهاب وتمويله بتشريعات الولايات المتحدة الامريكية سيما المتعلقة بمكافحة الارهاب يلاحظ حتما مدى تأثر المشرع بأحداث 11 سبتمبر 2001 ، حيث عرف مفهوم الارهاب تطور ملحوظ ، تطور ارتبط بخطورة الاعمال الارهابية وخطورة تناميها، ما دفع المشرع إلى التوسع في مفهوم الارهاب وتمويله إلى حد تجريم تشجيع أو تمويل الارهاب.

بالمقابل ورد مصطلح جرائم تمويل الارهاب في مصر في القانون رقم 8 لسنة 2015 بشأن الكيانات الارهابية والارهابيين على أنه" كل جمع أو تلقي أو حيازة أو إمداد أو نقل أو توفير أموال أو أسلحة أو ذخائر أو مفرقعات أو مهمات أو آلات أو بيانات أو معلومات أو مواد أو غيرها بشكل مباشر أو غير مباشر وبأية وسيلة كانت بما فيها الشكل الرقمي أو الالكتروني وذلك بقصد استخدامها كلا أو بعضا في ارتكاب أية جريمة إرهابية أو العلم بأنها ستستخدم في ذلك أو بتوفير ملاذ آمن لارهابي أو أكثر أو لمن يقوم بتمويله بأي من الطرق المتقدم ذكرها " .

وعليه فان تمويل الارهاب وفقا لمفهوم المشرع المصري لا يقف عند مجرد الدعم المالي أو المادي، سواء تمثل ذلك في مبالغ مالية، أو تحويلات، أو أماكن للايواء... إلخ؛ بل إن تمويل الارهاب يتحقق بالعديد من الوسائل الاخرى منها الدعم المعنوي من خلال الترويج والتحبيذ للاعمال الارهابية، كذلك من خلال التشجيع على هذه الاعمال بأي طريق، أو جمع الاموال للمنظمات، مع العلم بأغراضها. وهناك العديد من النصوص التي تجرم تمويل الارهاب سواء اتخذت الشكل الفردي أو التنظيمي[421] .

ويتضح من ذلك أن القانون المصري نص على وقف أنشطة الكيانات الارهابية وحظر اجتماعاتها وغلق الاماكن المخصصة لها كما حظر تمويل أو جمع الاموال للكيان سواء بشكل مباشر أو غير مباشر وتجميد أمواله وأموال أعضائه المستخدمة في النشاط الإرهابي[422].

---

[420] د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، مصدر سابق ، ص33 .

[421] د. إمام حسانين خليل، جرائم تمويل الارهاب في التشريع المصري، بحث مقدم إلى المؤتمر الرابع عشر للجمعية المصرية للقانون الجنائي حول تحديات العولمة والعدالة الجنائية، القاهرة، في الفترة من 19 إلى 20 مايو، القاهرة، 2009 ، ص1.

[422] خالد جمال حامد عبد الشافي، المواجهة التشريعية لظاهرة الارهاب، دراسة مقارنة، مصدر سابق، ص 5.

وفي ضـــوء ما ذكر يقترح الباحث تعريف تمويل الارهاب بأنه: (عملية تهدف إلى دعم وإمداد الافراد والجماعات الارهابية بالاموال، والمعدات، والادوات اللازمة لتنفيذ مخططاتهم الارهابية، وذلك أيا كان مصدرها، قانوني أو غير قانوني وهو يعلم بنية استخدامها للقيام بأعمال إرهابية). نظرا لان تمويل الارهاب يتم عن طريق إجراءات منظمة من قبل الممولين يتم من خلال هذه الاجراءات تمويل الاموال ســـواء أكانت هذه الاموال مشـــروعة أو غير مشـــروعة للجماعات أو المنظمات الارهابية للقيام بنشـــاطاتها، ويكون لتلك النشاطات آثار متعددة على الصعيد الامني والسياسي والاقتصادي والاجتماعي.

ثانيا : مصادر تمويل الإرهاب : تتعدد وتتنوع هذه المصادر إلى مصادر مشروعة وأخرى غير مشروعة، ومن الأمثلة الواضحة على المصادر المشروعة اســـتفادة هـــذه المنظّمات الإرهابية من نشاط العمل الخيري وخلافه لإيجاد مصدر مشروع لتمويل عملياتها، والمعيار لذلك هو بحسب ما إذا كانت تلك الأموال ناتجـةً من أموال تم الحصـول عليها بصـورة قانونية [423]، وعليه سـنبين المصـادر المشـروعة ومن ثم المصـادر غير المشروعة لتمويل الإرهاب وكالاتي :

1- تمويل الإرهاب عن طريق المصـــادر المشـــروعة : قد تُمول الجماعات الإرهابية من خلال أفراد أو جماعات، وقد تكون داخليةً أو خارجيةً، وقد يتم التمويل من خلال أموال التبرعات التي تجمعها المؤسسات الخيرية التي لا يخضع نشاطها لرقابة حازمة من قبل مؤسسات الدولة[424].

وبعد الحادي عشر من سبتمبر ٢٠٠١م اهتمت الأجهزة ذات الـــصلة بمكافحة الإرهاب وبعض الحكومات، مثـل الحكومـة الأميركيـة وبعـض الحكومات العربية، خصوصا تلك التي كان لها تجاربها في مجال مكافحـة الإرهاب، بموضوع الجمعيات والمؤسسات الخيرية ودورهـا فـي تمويـل الجماعات الإرهابية، حيث رجحت أن جزءا من أموال التبرعات من الممكن أن يتم توجيهه من قبل الجهات المتبرعة لدعم أنشطة إرهابية[425] .

وهناك العديد من المؤسسات والجمعيـات الخيريـة المنتـشرة فـي الولايات المتحدة الأميركية وفي غيرها من دول العالم، تم اتهامها بتمويـــل العمليات الإرهابية، وبناء على تلك الاتهامات تم إغلاق إحـــدى وأربعـــين مؤسسة خيرية في أنحاء العالم، أغلبها مؤسسات إسلامية وصنـــفت بأنهـــا مؤسسات تدعم الإرهاب، وهي مؤسسـة الأرض المقَدســـة" Land Holy Foundation " التي أغارت عليها المباحث الفيدرالية FBI" "وأغلقتها منذ ديسمبر العام ٢٠٠٠١م، ومن بين تلك المؤسسات المغلقة بعـد اتهامهـا بتمويل الإرهاب هيئة الإغاثة الإسلامية الأميركية "أيارا "[426].

ونظرا لاستخدام الجماعات الإرهابية بعض الجمعيـات والمؤسـسات الخيرية لتمويل أنشطتها الإرهابية، ولذا يتعين على البنوك أن تحـول دون استغلالها من قبل تلك الجمعيات والمؤسسات لتمويل الإرهاب، وذلك باتخاذ عدد من الإجراءات الوقائية في هذا الصدد بهدف عـدم إسـاءة اسـتغلال الجمعيات والمؤسسات الخيرية من جانب الجماعات والمنظمات الإرهابيـة، ومنع استغلالها كقنوات لتمويل الإرهاب، بما في ذلك غرض التهرب من تدابير تجميد الأموال، ومنع اســتغلالها كذلك لحجب أو إخفاء الغرض الســري من وراء تحويل الأموال لمنظمات إرهابية تحت ستار أغراض مشروعة[427].

---

[423] انظر: د . فضل يوسف إدريس، جريمة تمويل الإرهاب في القانون السوداني، بحث منشور في مجلـــة جامعـــة بحري للآداب والعلوم الإنسانية، السنة الخامسة، ع: (9) أغسطس ٢٠١٦، ص١٥٤.

[424] د. أحمد فتحي سرور ، مصـادر تمويل العمليات الإرهابية في الشـرق الأوسـط ، ط2 ، دار النهضـة العربية ، القاهرة ، 2018 ، ص 93 .

[425] د. سالم علي الظنحاني، الإطار القانوني لمكافحة تمويل الإرهاب "دراسة قانونية سياسية"، مصدر سابق، ص٥٩٧.

[426] د. سالم علي الظحناني ، المصدر نفسه ، ص 599 .

[427] وفي سبيل تحقيق هذه الأهداف تلتزم البنوك باتخاذ الإجراءات الآتية :

:١ - عدم فتح حساب خيري "محلي أو دولي" إلا بعد الحصول على موافقة من السلطات المختصة.

٢ - عدم فتح حسابات لمؤسسات مالية تعمل في مناطق مشبوهة.

ويرى الباحثُ أنّه لا ينبغي الهجوم على العمل الخيري الإسلامي لأنّه قد يكون أمرا مقصودا لذاته، كجزء من استراتيجية غربية شاملة للمواجهة المفترضة بين القوى الغربية والمسلمين والعالم الإسلامي.

2- تمويل الإرهاب عن طريق مصادر غير مشروعة : يرتبط تمويل جرائم الإرهاب بغيره من الجرائم الأخرى، مثل جرائم المخدرات والسلاح وغسيل الأموال "Laundering Money" ، ومن ثَم فإن التنظيمات الإرهابية كثيرا ما تعتمد في تمويلها على تلك النشاطات الإجرامية وغيرها للحصول على الدعم والتمويل المالي، فتعتمد تلك المنظّمات على نشاطات إجرامية مثل الاحتيال التجاري والاتجار بالمخدرات، والأسلحة والابتزاز والخطف وعمليات التهريب وتزييف العملة، وغسيل الأموال وغيرها من النشاطات الاجرامية [428].

وقد يتم تمويل الجماعات الإرهابية عن طريق أموال ناتجة عن ممارسة بعض الأعمال الإجرامية، وفي مقدمتها غسيل الأموال، فقد ثبت ان هناك علاقة وثيقة بين جريمة غسيل الأموال وجريمة تمويل الإرهاب ؛ إذْ أن الأساليب المستخدمة في غسيل الأموال هي نفسها بصورة أساسية تلك المستخدمة لإخفاء مصادر تمويل الإرهاب واستخداماته [429]، فالأموال التي يتم استخدامها في مساندة الجماعات والتنظيمات الإرهابية يمكن أن تنشأ عن مصادر مشروعة أو عن أنشطة إجرامية أو كليهما، غير أن تمويه مصدر تمويل الإرهاب يتسم بالأهمية بغض النظر عما إذا كان مصدره من منشأ مشروع أو غير مشروع، فإذا كان من الممكن إخفاء هذا المصدر فإنه يبقى متاحا للمزيد من أنشطة تمويل الإرهاب في المستقبل [430].

الفرع الثاني

اليات منع تمويل الإرهاب

يعد التمويل هو العصب الحقيقي للنشاطات الارهابية، فيتم الحصول على المواد ومن الممكن تجنيد الافراد وشراء ولائهم، لذلك حرص التشريعات على تجريم الدعم المادي والمالي للارهاب، حيث يأتي التمويل عادة من أفراد متعاطفين مع فكر تلك التنظيمات الارهابية، إلا أنهم لا يريدون الانخراط فيها حفاظا على وضعهم الاجتماعي والاقتصادي، فيقتصر دورهم على التمويل . وترجع أهمية مواجهة تمويل الارهاب، كون التمويل

---

٣ - عدم إجراء حوالات خارجية أو إصدار شيكات مصرفية أو شيكات سياحية، بناء على طلب الجمعيات الخيرية للخارج أو تلقي تبرعات لها من الخارج إلا بعد الحصول على موافقة السلطات المختصة.

٤ - عدم فتح حسابات بأسماء أي من رؤساء أو مديري الجمعيات والمؤسسات الخيرية بغرض إدارة أموالها، حيث يلزم أن تكون هذه الحسابات بأسماء تلك الجهات نفسها.

٥ - التحقق من مشروعية مصادر تمويل وأوجه إنفاق أموال الجمعيات والمؤسسات الخيرية.

٦ - الالتزام بتعليمات السلطات الأمنية الخاصة بحسابات الجمعيات والمؤسسات الخيرية.

انظر د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، مصدر سابق، ص٧٣-٧٤.

[428] فعلى سبيل المثال أبرمت جماعة" FARC" الإرهابية الكولومبية اتفاقًا مع عصابات تجارة المخدرات الكولومبية " Cartel The"بمقتضاه تم الاتفاق على أن تقدم الأولى الحماية اللازمة لتلك العصابات ضد الحكومة الكولومبية مقابل حصولها على حصة من أرباح تجارة الكوكايين، وقدر أن جماعة" FARC" حصلت بموجب ذلك الاتفاق على ما يقدر بـ ١٥٠ مليون دولار، أنفقت جماعة" FARC" معظم تلك المبالغ على التجنيد والتدريب للقيام بأعمال إرهابية، كما أصبحت تجارة المخدرات الأبرز والأكثر أهمية في تمويل الجماعات الإرهابية في أفغانستان، إذْ أن تلك الجماعات الإرهابية تشترط على تجار المخدرات أن يدفعوا لهم حصة من أرباحهم مقابل حمايتهم وعدم التعرض لهم وتأمين ممرات آمنة لهم .انظر: د. أسامة بن غانم العبيدي، جرائم تمويل الإرهاب وتطبيقاتها في النظام السعودي، مصدر سابق، ص١٤٢.

[429] د. سالم علي الظنحاني، مصدر سابق، ص596 .

[430] انظر: د. هشام عمر أحمد الشافعي، التعاون الدولي لمنع تمويل الإرهاب، بحث منشور في مجلة الفكر الشرطي، تصدر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مجلد (٢٥)العدد: (٩٧) ،أبريل ٢٠١٦ ، ص١١٩-١٢٠.

هو بمثابة الدماء في الجسم بالنسبة للعمليات الارهابية، حيث يأتي المال في مقدمة حاجيات التنظيمات الارهابية، سواء لاعداد عناصرها وتدريبهم، أو توفير الوسائل اللوجستية من حيث الاقامة، والملبس والمأكل، والتنقل، أو اقتناء الاسلحة والمتفجرات [431].

وقد اتخذت دول العالم إجراءات مختلفة لتجفيف منابع الارهاب في محاولة منها لخنق الظاهرة الارهابية والحد منها ومحاصرتها ،حيث اتخذت الدول والمنظمات الدولية مجموعة من الاجراءات الهادفة إلى وضع آليات مواجهة التمويل الارهابي محليا وإقليميا ودوليا ، وذلك لتطوير التشريعات المتعلقة بمكافحة الإرهاب ومنع تمويله وتجفيف منابعه ، بعد ان اخذ تمويل الإرهاب حيزا كبيرا من الاهتمام في كافة انحاء العالم [432] . وابرز الاليات المعتمدة للقيام بهذا الدور هي مايأتي :

أولا : تجميد أموال الارهابيين والتنظيمات الإرهابية : بذلت جهود دولية لمكافحة تمويل الارهاب، أهمها تلك الجهود التي قامت بها المجموعة الدولية للعمل المالي، وتوصلت من خلالها إلى تسع توصيات مهمة في هذا الصدد موجهة إلى الدول لكي تأخذها في اعتبارها عند اتخاذها إجراءات مكافحة تمويل الارهاب، كما توصلت بعض المؤتمرات الدولية ومنها المؤتمر الدولي لمكافحة الارهاب الذي عقد بالرياض عام 2005 ، إلى عدد من التوصيات التي تتعلق بهذا الموضوع. ويجب على كل بلد الاخذ بالمعايير الفورية لتطبيقها، وتنفيذ كل القرارات الصادرة عن الامم المتحدة عام 1999 الخاصة بالضغط على التمويل الارهابي، بما فيها قرار مجلس الامن رقم 2001/1373 ، وعلى كل دولة اعتماد تجريم جزئي للتمويل الارهابي والانشطة الارهابية والمنظمات الارهابية؛ على أن تبادر الدول إلى وضع هذا الجرم ضمن إطار الاعمال الإرهابية [433] .

وعلى كل دولة أن تتعاون مع الدول الاخرى وفق معاهدات أو اتفاقات أو آليات أخرى في مجال التنسيق القضائي أو تبادل المعلومات، والمساعدة القصوى في إطار التحقيقات والأبحاث أو التدابير الجزائية المدنية أو الحكومية المتضمنة التمويل الارهابي للانشطة والمنظمات الارهابية؛ وعلى الدولة اتخاذ كل الاجراءات الممكنة كي لا تكون ملجأ للافراد الملاحقين بتمويل الارهاب والانشطة والمنظمات الارهابية، وعليها تطبيق التدابير التي تخولها تسليم هؤلاء الافراد[434] .

ومن خلال هذه الفقرة نلاحظ بانه من اللازم للقيام بها ان تقوم الشركات المالية بالافصاح عن بيانات زبائنها المعنين في هذه الفقرة دون ان تتم مسائلتها قانونا ، كون الامر متعلق بالامن القومي والهدف منه الحد من استفحال المنظمات الإرهابية والإرهابيين .

ثانيا : مراقبة وتنظيم الاعمال المصرفية وأنشطة الجمعيات والمؤسسات الخيرية الخاصة : قد يقوم التنظيم الارهابي بجمع التبرعات تحت ستار توزيعها على الفقراء والمحتاجين، ولكنه يمضي إلى استخدامها في أغراض الجرائم الارهابية، وذلك قد يتم عن طريق الافراد أو عن طريق مؤسسات معينة ترتبط بالتنظيم الارهابي. ومن المعروف أن المؤسسات العاملة في ميدان العمل الاجتماعي تمر بعدة مراحل فيما يتعلق بتمويل المشاريع، بداية من التبعية، وصولا الى الاعتماد على الذات، أو الاعتماد المتبادل كمرحلة عليا، وإحداث الشراكة مع الجمعيات والمنظمات الأخرى [435] .

---

[431] د. محمد السيد عرفة، تجفيف مصادر تمويل الارهاب، مصدر سابق، ص105 .

[432] د. عصام عبد الفتاح عبد السميع مطر، الجريمة الارهابية، مصدر سابق، ص35.

[433] د. محمد السيد عرفة، تجفيف مصادر تمويل الارهاب، مصدر سابق، ص136 .

[434] د. أسامة عبد المنعم علي إبراهيم، حصر ومكافحة غسل الاموال ومكافحة تمويل الارهاب والنقل غير المشروع للاموال عبر الحدود في التشريعات العربية، مصدر سابق، ص 130.

[435] د. عصام عبد الفتاح عبد السميع مطر، الجريمة الارهابية، مصدر سابق، ص63 .

ويشـــير الباحث هنا إلى أن التبرع قد يكون من مصـــادر تمويل الجرائم الارهابية، والامر لا يخرج عن أحد احتمالين نوضحهما تباعا :

1- الاحتمـال الاول: أن يتجـه اســـتخدام الاموال التي يتم جمعهـا عن طريق التبرع إلى تحقيق أغراض إرهابية دون أن يعلم المتبرعون الاصـليون الوجهة الحقيقية التي تصـرف فيها أموالهم؛ كأن يسـتغل التنظيم الارهابي النزعة الدينية لدي البعض؛ ومن ثم يتم حثهم على التبرع لمســـاعدة المحتاجين، أو القيام ببناء دور للعبادة... الخ، ثم يوجهون تلك الاموال لشـراء الاسـلحة والمتفجرات والصـرف على النشـاط الارهابي؛ وقد يتم اسـتخدام الاموال التي تم جمعها في أنشـطة تجارية مربحة تدر اموالا يتم اسـتخدامها في تمويل أنشـطة إرهابية بعد ذلك، ومن ثَم تضـليل مصـدر الاموال وطمأنة المتبرعين [436].

2- الاحتمـال الثـاني: أن يتم اســـتخدام الاموال التي يتم جمعهـا من خلال المتبرعين الذين هم في الوقت نفسـه على علم بالوجهة الحقيقية التي سيتم صـرف أموالهم فيها، وهي القيام بنشاط إرهابي، وفي هذه الحالة فان المتبرع يكون من المتعاطفين مع التنظيم الإرهاب [437] .

أي قد يأتي التمويل من تبرعات ومســـاعدات الاثرياء المتعاطفين والمؤيدين للفكر الارهابي، والذين يدفعون بسخاء لتمويل العمل الارهابي بوصـفهم جزءا من المنظومة الارهابية ويتحملون كل المسؤولية عن كل عمل إرهابي يتم التخطيط له ، ثم يتم تنفيذه [438] .

ويلاحظ أن التمويل في الكثير من المنظمات الارهابية يأتي من جانب فرد، أو مجموعة من الافراد المتعاطفين مع التنظيم الارهابي، ويحمل فكرة الارهابي نفسـه؛ حيث يكون الشـخص الممول يملك التوجهات نفسها؛ وفي هذا الصدد فان ممول التنظيم الارهابي يكون مساهما في الجريمة ومشاركا فيها[439] .

ولا يختلف الامر هنا اذ انه من اللازم على الشركة البوح عن بيانات هؤلاء للجهات المعنية من اجل مراقبتهم ، ومعرفة حركة الأموال الخاصة بهم نظرا للخطورة التي يشكلونها على الامن والاستقرار المحلي والدولي ، ولا يشكل ذلك أي خرق للالتزام بالمحافظة على البيانات الشخصية للزبائن .

ثالثا : تبادل المعلومات بشـأن مكافحة جريمة تمويل الإرهاب : إن الجرائم الارهابية تكتسـب الصـفة الدولية، فهي ترتكب من عناصـر ذي جنسيات مختلفة، ويتخذ التخطيط والاعداد لها وتنفيذها والفرار من عقوبتها من أقاليم أكثر من دولة مسرحا له ، لذلك فانه لا وطن للارهاب ولا هوية محددة لمرتكبي جرائمه [440].

وهذه الصـفة السـابقة للارهاب تجعل آثاره متناثرة في دول متفرقة متباعدة، ولا سـبيل إلى اكتمال الصـورة الموصلة إلى تحديد هوية ووجهة العناصر الارهابية سوى بتجميع تلك الاثار المتناثرة التي يخلفها الارهابيون وراءهم، وهو مـا يتعذر تحقيقه إلا بالتعاون الصـــادق والجاد بين الاجهزة الامنية في الدول التي يتخذ زبانية الارهاب من أراضـيها مسـرحا لخطوة او اكثر من خطوات عملياتهم الارهابية، ولو كانت موجهة في النهاية إلى دولة بعينها[441].

---

[436] د. علي حامد علي الخولي ، مكافحة تمويل الإرهاب ، بحث منشـور في مجلة الحقوق ، تصـدر عن جامعة الإسـكندرية المجلد 1 ، العدد 4 السنة 2018 ، ص1594 .

[437] د. عصام عبد الفتاح مطر، مصدر سابق، ص16.

[438] د. حسن محمد ثاني، سيكولوجية الارهاب، مكتبة عالم الكتب، القاهرة، 2006 ، ص 156.

[439] د. يوســف بن أحمد الرميح، تمويل الارهاب، طرق ملتوية وأســاليب قد تخفي على البعض، جريدة الاقتصـــاد أون لاين 2007 على الموقع الاتي : http://www.aleqt.com.

[440] د. علي حامد علي الخولي ، مصدر سابق ، ص1603 .

[441] د. محمد مؤنس محب الدين، الارهاب في القانون الجنائي على المستويين الوطني والدولي، دار النهضة العربية، القاهرة، 1998 ، ص180.

وأكثر ما يتجسد فيه هذا التعاون الامني هو مجال "الانظمة المعلوماتية". فتزود أجهزة الامن في الدول المعنية بالارهاب الاجهزة النظيرة لها في الدولة المعتدى على أمنها وسلامتها أو المهددة بخطر هذا الاعتداء بكل ما في جعبتها من معلومات تفيد في التوصل إلى كشف هوية الارهابيين وأماكن اختفائهم وما يخططون ويدبرون له من عمليات مستقبلية [442].

ولا يكون هذا التبادل في المعلومات بين الاجهزة الامنية فعالا ومؤثرا في مجال مكافحة الارهاب، ما لم يتم من خلال قنوات متحررة من كل أشكال ومعوقات الروتين ، حتى وان كان هذا المعوق هو تحت غطاء المحافظة على الخصوصية وحماية البيانات الشخصية ، كون صاحب هذه البيانات اما ان يكون مذنبا ولا يستحق هذه الحماية ، او يكون موضع شك ومن الضروري العمل على تحقيق الطمأنينة والاستقرار وهذا هو الهدف الأولى حتى وان كان فيه نوع من المساس بحق فردي غير مقصود لذاته .

رابعا : الضوابط المصرفية والمالية على حركة انتقال الأموال :يتضح من قوانين وأنظمةُ مكافحة تمويل الارهاب في الدول المختلفة، ان أهم الاجراءات التي تتخذها الدول لمنع وقوع جرائم تمويل الارهاب والوقاية منها إجراءات الرقابة الداخلية التي تقوم بها البنوك التجارية وأنظمة إدارة الاخطار الاخرى، كما أن هناك إجراءات للرقابة الدولية على حركة انتقال الاموال عبر الحدود الدولية. إذ أنه من المستقر عليه أن هناك قواعد مصرفية تنظيمية تُحدد كيفية أداء العمل المصرفي عند التطبيق في الدول ُالمختَلفة، وغالبا ما يكون هذا التحديدُ باسناد الاشراف والتوجيه والرقابة على العمل المصرفي في جميع المصارف للبنك المركزي في الدولة؛ الذي يُطلق عليه عادة تسمية "بنك الدولة" أو "البنك الوطني" أو " مؤسسة النقد " أو" البنك المركزي" كما هو عليه الحال في العراق ، وهو الذي يكون الموجه لانشطتها والمراقب لاعمالها، ولكافة البنوك الاخرى العاملة في الدولة، بحيث تسير السياسة المصرفية في إطار ديناميكي محكم [443] .

وهناك مجموعة من القواعد التي تقوم بها البنوك والتي تمثل الحد الأدنى من الضوابط التي يجب ان تلتزم بها [444] ، وهي كالاتي :

1- التزام المصارف بعدم التدخل في أية عملية بنكية ذات صلة بالارهاب أو الارهابيين، حيث يمتنع عليه التدخل فيها بأي شكل من الاشكال .
2- إمداد البنك المركزي البنوك التابعة له بالمعلومات اللازمة لمكافحة تمويل الارهاب من خلال تزويد جميع المصارف العاملة بالدولة بقائمة بأسماء الاشخاص الارهابيين، والجماعاتُ والمنَظمات الارهابية، وكذلك الاشخاص الذين لهم صلة بتلك الجماعات والمنظمات .
3- تلتزم المصارف بأن لا تفتح أي حساب أو تُبرم أية عملية لافراد أو منشآت غير مقيمة إقامة قانونية بالدولة.
4- التزام المصارف والمؤسسات المالية العاملة بالدولة بالاحتفاظ بالسجلات والمستندات المتعلقة بعملياتها ومعاملاتها مع زبائنها وفقا للاجراءات المصرفية المعتادة؛ وذلك لكي يسهل الرجوع إليها عند الحاجة، سواء من قبل البنك نفسه أو من قبل الجهات الرقابية والاشرافية .
5- تنظيم عمليات التحويل المالي (الحوالات- الصكوك- الاعتمادات المستندية – الاستثمار .. الخ) ، عبر المصارف، وذلك حتى يمكن تتبع الاشخاص المشبوهين قبل تنفيذ العملية .

---

[442] د. عصام عبد الفتاح مطر، مصدر سابق، ص20 .
[443] د. نسرين محسن نعمة الحسيني و الدكتور محمد حسن مرعي ، الجرائم الالكترونية الواقعة على الاموال ، المكتب الجامعي الحديث ، مصر ، 2020 ، 263 .
[444] د. محمد السيد عرفة، تجفيف مصادر تمويل الارهاب، مصدر سابق، ص371 وما بعدها.

6- التزام المصارف وفروعها بنصوص القوانين واللوائح المصرفية والتعليمات التي تصدرها الجهات الرقابية والامنية، فيما يتعلق بفتح الحسابات والتعامل مع المؤسسات والافراد[445] .

وهناك إجراءات يجب القيام بها في حالة كشف مؤشرات مشبوهة وهي [446] .

1- استخدام جميع الوسائل المتاحة لمتابعة المعاملات والصفقات المشبوهة من خلال التقارير وعلى سبيل المثال قائمة الدول غير الممتثلة للمعايير الدولية وقائمة الافراد والكيانات في القوائم الدولية الصادرة عن الأمم المتحدة ولجنة تمويل أموال الارهابين .

2- متابعة اخر التطورات بشأن اتجاهات مكافحة غسيل الأموال وتمويل الإرهاب وإجراءات مكافحته وخاصة فيما يتعلق بهذا المجال مايتم إصداره من مجموعة العمل المالي وصندوق النقد الدولي ، والبنك الدولي ، ولجنة بازل والمنظمات الدولية الأخرى .

3- الاخذ بعين الاعتبار القضايا التالية في إدارة الحسابات الخاملة وعلى النحو الاتي :

أ- تحديد فترة محددة للحسابات الخاملة وبعد انتهاء هذه الفترة تحال هذه الحسابات الى الإدارة الرئيسية .

ب- ينبغي ان لا يتم اجراء أي مدفوعات لهذه الحسابات مالم يكن هناك موافقة من مدير الفرع او من ينوب عنه .

4- برمجة نظام الي لاعداد الابلاغات التي تساعد في تعزيز فعالية النظام الداخلي في مجال مكافحة غسيل الأموال وتمويل الإرهاب للكشف عن المعاملات المشبوهة والابلاغ عنها وتشمل على سبيل المثال لا الحصر ما يلي :

أ- أي شبهة في حركة حسابات وارصدة كل من العملاء والموظفين لتشمل كل حساب خلال فترة محددة ، والرصيد خلال كل شهر ، ومعدل الرصيد ، وعدد المعاملات التي يتم اجراؤها ، وذلك من اجل رصد أي نشاط لحساب غير طبيعي .

ب- أي شبهة في التحويلات ، بما فيها الوارد والصادر ، والداخلي والخارجي ، ومبلغ كل منها ، والعملة التي تم تحويلها وطريقة الدفع سواء كانت نقدا او بشيك (صك) ويفترض ان يتم تنفيذها لكل عميل بشكل منفصل .

ت- الإبلاغ عن أي شبهة في حركة ورصيد حسابات البنوك الخارجية ، حيث يجب ان تسمل الحوالات التي تم اجراؤها باي وسيلة كانت والمبلغ والعملة المحددة ، واسم البنك ، والمستفيد الحقيقي ، فضلا عن عدد وحجم المعاملات التي يتم تنفيذها مع كل المصارف الخارجية ، واي تغييرات أخرى .

وقد اهتمت التشريعات المقارنة بايقاع اقصى العقوبات على مرتكبي جريمة تمويل الإرهاب ، ففي العراق فقد ذهب المشرع العراقي في المادة 37 من قانون مكافحة غسيل الأموال وتمويل الإرهاب الى إيقاع عقوبة السجن المؤبد على كل من ارتكب جريمة تمويل الإرهاب . اما في الاتحاد الأوربي و بعد أحداث الحادي عشر من سبتمبر وتحديدا وفي ٢٨ سبتمبر ٢٠٠١ ، اعتمد الاتحاد الأوروبي خطة عمل لمكافحة الإرهاب، تتضمن سلسلة واسعة من التدابير يتعين اتخاذها في مختلف القطاعات (التعاون القضائي، التعاون بين أجهزة الشرطة، سلامة وسائل النقل، مراقبة الحدود وتأمين الوثائق، مكافحة التمويل، الحوار السياسي والعلاقات الخارجية، والدفاع ضد هجمات الأسلحة البيولوجية والكيميائية والمشعة والنووية . وقد أدت العمليات الإرهابية في مدريد في مارس ٢٠٠٤م ولندن في يوليو ٢٠٠٥ ،إلى تكثيف التعاون في مكافحة الإرهاب في الاتحاد الأوروبي، وإكمال خطة العمل بإضافة المزيد من التدابير والإجراءات إليها، وقد اعتمد المجلس الأوروبي الذي انعقد في ٢٥ مارس ٢٠٠٤ إعلانًا حول التضامن ضد الإرهاب ، يفرض واجب تقديم الدعم

---

[445] مثالها الدليل الارشادي الخاص بمؤشرات الاشتباه في عمليات غسل الأموال وتمويل الإرهاب لسنة 2017 الصادر من البنك المركزي العراقي .

[446] الدليل الارشادي الخاص بمؤشرات الاشتباه في عمليات غسل الأموال وتمويل الإرهاب لسنة 2017 الصادر من البنك المركزي العراقي .

بكل الأدوات المتاحة، بما في ذلك الموارد العسكرية للدولة العضو في الاتحاد التي تتعرض لهجوم إرهابي[447] .

وفي ٢٠١٦م اقترحت المفوضية الأوروبية بشكل خاص تدبيرا جديدا يتيح على الدوام اعتبار تمويل الارهاب جريمة جزائية، والعمل على «سد الثغرات» في القوانين الوطنية لكل بلد في هذا المجال، كما اقترحت المفوضية تدبيرا جديدا يعزز الرقابة على حركات الأموال السائلة بما يتعلّق بالأشخاص الذين يدخلون الاتحاد الأوروبي أو يخرجون منه وبحوزتهم عشرة آلاف يورو على الأقل، كما اقترحت توسيع «الرقابة الجمركية لتشمل أيضا المال السائل المرسل عبر الطرود البريدية أو عبر الشحن، ومراقبة تحرك الأحجار الثمينة والذهب«، كما قدمت المفوضية أيضا اقتراحات لتحسين "نظام شنغن للمعلومات" ، وهو عبارة عن نظام لتقاسم المعلومات بين السلطات القضائية والشرطة بشكل خاص لدى الدول الأوروبية. وتم الدخول إلى هذا النظام نحو ثلاثة مليارات مرة عام ٢٠١٥ وهو يستخدم خاصة لإدارة الحدود الأوروبية. والهدف هو زيادة فعالية هذا النظام في مجال مكافحة الإرهاب [448] .

ومما سبق يرى الباحثُ أن هذه القواعد والإجراءات تشكل آليةً أو وسيلةً فعالة لعرقلة تمويل الجماعات الإرهابية، ويمكن إجمال مدى أهمية هذه القواعد والإجراءات في مكافحة تمويل الإرهاب، وذلك على النحو التالي .

1- إن تلك القواعد تتيح للسلطات الوطنية في الدول الأعضاء تجميد الأصول المعرضة لخطر نقلها فجأة إذا لم يتخذ أي إجراء في شأنها .
2- تُعتبر هذه القواعد والإجراءات خطوة مهمة على طريق إزالة الوسائل المتاحة للإرهابيين.
3- إن هذه التدابير من شأنها مساعدة السلطات على تتبع التدفقات المالية بشكل أفضل وتعطيل تمويل الشبكات الإجرامية .
4- لا خلاف على أن هذه الإجراءات والقواعد ستحقق الهدف الذي وضعت من أجله، وهي: منع استخدام النظام المالي لتمويل الأنشطة الإجرامية ومنها تمويل الإرهاب، وكذلك تعزيز قواعد الشفافية للحيلولة دون إخفاء الأموال على نطاق واسع، والذي يؤدي في النهاية إلى إغلاق الطريق أمام تمويل الأنشطة الإجرامية دون إعاقة الأداء العادي للأسواق المالية ونظم الدفع، فضلاً عن تحقيق التوازن بين الحاجة إلى زيادة الأمن وحماية الحقوق الأساسية والحريات الاقتصادية [449] .

اما بخصوص مصر فمن المتعارف عليه انها عانت من الانشطة الارهابية، وخاصة في الفترة الأخيرة ، ومن ثم فمن حق الدولة تواجه الارهاب استخداما لحقها في الدفاع عن سيادتها وأمنها ، واستقرارها وسائر حقوق مواطنيها ، باعتبار أن مواجهة الإرهاب تهدف اساسا لحماية حقوق الانسان[450]، ومن ناحية أخرى فان الارهاب يمثل اعتداء على القانون، ولا يمكن رد هذا الاعتداء إلا بالقانون كما أن تطبيق الاحكام الإجرائية التي تضمنها قانون مكافحة الارهاب المصري لسنة 2015 ، فقد تضمن تعديل التشريعات للاحكام الإجرائية المتعلقة بالإرهاب ويلحق بها جريمة تمويل الإرهاب [451] .

---

[447] د. إلياس أبو جودة: الإرهاب والجهود الدولية والإقليمية لمكافحته، مجلة الجيش، لبنان، العدد (91) كانون الثاني ٢٠١٥، ص18 .
[448] د. نسرين محسن نعمة الحسيني ن د. محمد حسن مرعي ، مصدر سابق ، ص 127 .
[449] د. أسامة عبد المنعم علي إبراهيم ، مصدر سابق ، ص157 .
[450] د. إمام حسنين، جرائم الارهاب الدولي في التشريعات المقارنة، مصدر سابق، ص 3 وما بعدها.
[451] د. علي حامد علي الخولي ، مصدر سابق ، ص1611.

وقد عاقب المشرع المصري على تمويل الارهاب بالسجن المؤبد، حيث نصت المادة (13) من قانون مكافحة الارهاب المصـري رقم 94 لسـنة 2015 على أنه: يعاقب بالسـجن المؤبد كل من ارتكب جريمة من جرائم تمويل الارهاب إذا كان التمويل لارهابي وتكون العقوبة الاعدام إذا كان التمويل لجماعة إرهابية أو لعمل إرهابي. وفى الاحوال التي ترتكب فيها الجريمة بواسطة جماعة إرهابية يعاقب المسؤول عن الادارة الفعلية لهذه الجماعة بالعقوبة المقررة في الفقرة السابقة من هذه المادة ما دامت الجريمة قد ارتكبت لحساب الجماعة أو لمصـلحتها. كما تعاقب الجماعة الارهابية بغرامة لا تقل عن مائه ألف جنيه ولا تجاوز ثلاثة ملايين جنيه وتكون مسؤوله بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات .

ومن الواضح أن المشرع المصري قد أنشأ جريمة خاصة بتمويل الارهاب. وتبدو الحكمة من هذا التجريم الخاص من عدة نواح، أهمها: إدراك مدى الخطورة البالغة التي تنطوي عليها ظاهرت تمويل الارهاب وما ترتبه من آثار اقتصادية واجتماعية وأمنية، والاخذ في الاعتبار أن أسلوب الجزاء الجنائي المتمثل في العقوبة الرادعة هو الملجأ الاخير لمواجهة الاجرامية بالغة الخطورة التي تهدد كيان المجتمع وأمنه؛ فضـال الظواهر عن أن الاتفاقيات الدولية التي وقع عليها العديد من دول العالم في مجال مكافحة الجريمة المنظمة بصفة عامة وجريمة غسيل الاموال ومكافحة الارهاب بصفة خاصة عليها تلزم الدولة الموقعة والمصدقة عليها باللجوء إلى أسـلوب التجريم والعقاب التجريم لمواجهة عمليات غسـيل الاموال، كما هو الحال في الاتفاقية الدولية لمكافحة تمويل الإرهاب [452] .

المطلب الثاني

القيود المفروضة بسبب طبيعة المعاملة

يجري الزبون العديد من المعاملات مع الشـركات المالية ، سـواء في الإيداع او السـحب او الاسـتثمار ، او التحويل ، وتعد المعاملة الأخيرة واحدة من اكثر المعاملات التي تثير الإشـكاليات مع الالتزام بحماية البيانات الشخصية وخصوصا في بعض الالتزامات التي يرتبها عقد التحويل الالكتروني ، وعليه سنقسم هذا المطلب على فرعين في الأول نتناول تعريف التحويل الالكتروني والثاني سنبين فيه مورد الخروج على الخصوصية في التحويل الالكتروني مبينين فيه مدى التعارض مع الالتزام بحماية البيانات الشخصية للزبائن وكالاتي :

الفرع الأول

تعريف التحويل المالي الالكتروني

من اجل تحديد معنى التحويل المالي الالكتروني لابد من تعريفه اصطلاحا والذي يستلزم التوقف على ما سيق لـه من تعريفات في نطاق الفقه القانوني لنعرج بعدها الى تعريفه في النطاق التشـريعي أولا ، ومن ثم بيان التعريف في الاصطلاح وكالاتي :

أولا : التعريف الفقهي : تعددت وجهات الفقه بخصـوص تحديد مفهوم "التحويل المالي الإلكتروني"، وكان مرد هذا التعدد هو الاختلاف في تحديدهم لطبيعته القانونية، فمنهم من كيفه على أنه عقد - كما سـنرى - وعرفه وفقاً لذلك على أنه "عقد بين الآمر بالتحويل المالي والبنك مصدر الحوالة، يتم انعقاده أو تنفيذه كله أو جزء منه باستخدام وسيلة اتصال عن بعد، يلتزم بموجبه البنك بأن يدفع بنفسه أو بواسطة غيره مبلغاً من النقود يعادل قيمة الحوالة إلى المسـتفيد من الحوالة مقابل عمولة متفق عليها[453]، أي إن التحويل المالي

---

[452]د. خالد سري صيام، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالثقة العامة وجرائم الارهاب وتمويله، الطبعة1، 2006م، ص 106.نقلا عن د. محمد السيد عرفة، تجفيف مصادر تمويل الارهاب، مصدر سابق ، ص 376 .

[453]د. محمد عمر ذوابة، عقد التحويل المصرفي الإلكتروني، دار الثقافة للطباعة والنشر، الأردن، ٢٠٠٦م، ص٢٤

الإلكتروني هو عقد كبقية العقود، لا يختلف عنها إلا في أسلوب تنفيذه ، ويؤخذ على هذا التوجه أنه يعود بعملية التحويل إلى الأفكار التقليدية في القانون المدني ، مما يستلزم توافر الأركان العامة للتعاقد من الرضا والأهلية والمحل والسبب في كل عملية تحويل يجريها الزبون .
والحقيقة أن هذه الأفكار التقليدية الذي تبناها هذا التوجه - كما يرى البعض لا تميز بين أمر التحويل والتحويل نفسه، فالتحويل تقنية تختص الشركة او المؤسسة المالية بالقيام بها بناء على الأمر الصادر من طرف الزبون، وهذا الأمر قد يأتي في عدة أشكال، فقد يسمح للزبون بإصدار بعض أوامر التحويل دون حاجة إلى إبرام عقد خاص بخصوصها؛ لأنه بمجرد القيام بفتح حساب للزبون، تلتزم بحد أدنى من الخدمات تقدمها له، من بينها بعض خدمات الخزينة [454].

لكن في المقابل قد يتطلب إصدار بعض أوامر التحويل الأخرى إبرام عقد خاص بين الطرفين ينظم العلاقة بينهما، خاصة فيما يتعلق بتحديد شروط وحالات وكيفية إصدار تلك الأوامر وتنفيذها، إلا أن ذلك لا يجعل من العملية بحد ذاتها عقداً، فالعقد يتم إبرامه لتنظيم العلاقة بين الطرفين بشكل يسبق إجراء عملية التحويل المالي الإلكتروني ذاتها ، لهذا نجد أن الفقه الذي يأخذ بالاتجاه الحديث في تكييفه لعملية التحويل، تعددت تعريفاته له، فمنهم من عرفه بأنه: (منح الصلاحية لمؤسسة مالية ما، للقيام بحركات التحويلات المالية الدائنة والمدينة من حساب بنكي إلى حساب بنكي أخر، أي إن عملية التحويل تتم إلكترونياً عبر الهواتف وأجهزة الكمبيوتر وأجهزة المودم عوضاً عن استخدام الأوراق)[455].

ويعرفه البعض بأنه: (تعليمات يصدرها الزبون إلى مصرفة بنقل مبلغ نقدي من حسابه إلى حساب المستفيد باستخدام الوسائل الإلكترونية) [456]، ويعرفه البعض: " بأنه التحويلات الإلكترونية للاعتمادات النقدية التي تتم الكترونياً بصفة كلية داخل أنظمة الدفع الشائعة فيما بين البنوك [457]. وعرفه البعض بأنه: "استخدام التقنيات الإلكترونية في خطوة أو أكثر من خطوات العملية التي كانت تتم فيما سبق لإتمام التحويل باستخدام الورق [458] .

ويعرفه البعض بأنه "عملية تحويل الأموال من خلال وسيلة إلكترونية أو اتصال أو حواسيب أو أشرطة مغناطيسية بهدف إعطاء التعليمات أو الصلاحيات لمؤسسة مالية لإيداع أو سحب الأرصدة من حساب ما [459]. ويبدو لنا أن هذا التعريف الأخير منتقد من ناحيتين؛ الناحية الأولى: أنه قصر وظيفة التحويل على الإيداع والسحب من الحساب رغم أنهما ليستا من وظيفته، التي تهدف إلى تحويل الأموال بين الحسابات بأية وسيلة إلكترونية تمكن من إجراء التحويل. والناحية الثانية: أنه لم يحدد ما إذا كان يمكن إجراء التحويل بالطرق الإلكترونية بين حسابين للزبون ذاته أو لزبون آخر في البنك نفسه أو بنك آخر . وهناك من يعرف التحويل الإلكتروني في مجال التجارة الإلكترونية بأنه " الدورة الإلكترونية المأمونة والسريعة لنقل الأموال

---

[454] د. محمود أبو فروة ، مسؤولية البنك المدنية في عمليات التحويل الالكتروني، دار وائل للطباعة والنشر والتوزيع، الأردن، عمان، ٢٠١٤م، ص ٢٨ ،٢٩.
[455] د. سعد غالب التكريتي، بشير عباس العلاف، الأعمال الإلكترونية، دار المناهج، الأردن، بدون تاريخ نشر، ص ٣٣٦.
[456] Mpakwana Annastacia Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, Journal of International Commercial Law and Technology Vol. 5, Issue 4 (2010), p.202.
[457] Geoffrey Turk; money and currency in the 21 st Century, July 1997p.1. Available at: http://web.archive. org/ web/ 20010410032230/ http:/www. goldmoney. com/ futuremoney. html.
[458] د. بلال عبد المطلب بدوي ، الالتزام بالافصاح عن المعلومات في سوق الأوراق المالية ، دار النهضة العربية ، القاهرة ، 2006 ، ص ٦٦.
[459] د. راجي عبد الملك، دراسة شرعية وقانونية لوسائل ونظم الدفع الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهره، ٢٠١٠م، ص٦٦.

من المشـتري إلى البائع عبر المؤسـسـات المالية وبأقل تكلفة ممكنة [460]. والملاحظ على جميع التعريفات السابقة أنها ركزت على الوسيلة المستخدمة في عمليات التحويل المالي دون أن تتناول مضمون تلك العمليات وطبيعتها القانونية، الأمر الذي يقودنا إلى التساؤل عن المفهوم القانوني لعمليات التحويل المالي الإلكتروني.

ثانيا : التعريف التشـريعي :نظم التحويل المالي في اغلب التشـريعات المتقدمة [461]، في لم ينظم المشـرع العراقي عمليات التحويل المالي الإلكتروني بشكل مستقل عن العمليات المصرفية الإلكترونية المختلفة، ولكنه أورد تعريفا خاصـا للتحويل المصـرفي في المادة (258 / 01) من قانون التجارة العراقي لسـنة 1984 ، اذ نصـت على أن " النقل المصـرفي عملية يقيد المصـرف بمقتضـاها مبلغا معينا في جانب المدين من حسـاب الآمر بالنقل بناءا على أمر كتابي منه وفي الجانب الدائن من حساب الآخر " كما نصت المادة (01/329) من قانون التجارة المصـري لسـنة 1999 على أن " النقل المصـرفي عملية يقيد البنك بمقتضـاها مبلغا معينا في الجانب المدين من حسـاب الآمر بالنقل بناءا على أمر كتابي منه وفي الجانب الدائن من حسـاب آخر .... " .
من خلال النصين السابقين يتضح أن التحويل المصرفي يفترض وجود حسابين تنتقل النقود من أحدهما عن طريق القيد في هذين الحسـابين ، حيث يقيد المبلغ المطلوب نقله في الجانب المدين للأمر و في الجانب الدائن للمستفيد ، و تأسيسا على ما سبق فقد ذهب جانب من الفقه إلى أنه عند عدم وجود حسابين فإن العملية عندها لن تكون عملية تحويل مصرفي وانما قد تكون وكالة في الوفاء[462].
إن ما جاء في تعريف التحويل المصـرفي يخالف الواقع العملي للعملية المصـرفية ، حيث أن التحويل المصـرفي في البنوك لا يشـترط فيه توافر حسـابين لكل من الآمر و المسـتفيد ، فقد يقدم البنك خدمة التحويل المصـرفي لغير زبائنه الدائمين وهؤلاء لا يحتفظون بحسـابات لدى البنك مقدم الخدمة ، وعليه فإن اشـتراط توافر الحسابات سيخرج تلك العملية من أن تكون تحويلا مصرفيا وهذا خلافا لما هي عليه . فهناك من صور التحويلات المصرفية (وخاصة الحوالات المصرفية السريعة أو الفورية) ما تتم عند صندوق البنك المحول من قبل زبون غير دائم للبنك لا يملك حسـابا لدى البنك بحيث يتم دفع مبلغ الحوالة لصـندوق البنك الذي بدوره يسلم ما يعادل قيمتها للمستفيد نقدا ، فإذا لم تعتبر هذه العملية تحويلا مصـرفيا استثناءا من النصـوص التشريعية أعلاه فسيكون من الصعب ايجاد التكييف الصحيح .

وعرفه القانون النموذجي للتحويلات الدولية للأموال Crédit international lawon model الصـادر في 1992 عن لجنة الأمم المتحدة المعروفة . uncitral يعرف هذا القانون التحويل المالي بأنه مجموعة العمليات التي تبدأ بأمر الدفع الصادر عن الأمر بهدف وضع قيمة الحوالة تحت تصرف المستفيد ، ويشمل التعريف أي

---

[460] د.عبد الرحيم الشـحات البحطيطي، المخاطر المالية في نظم المدفوعات في التجارة الإلكترونية كأحد التحديات التي تواجه النظم المصـرفية، بحث منشـور في مجلة جامعة الملك عبد العزيز، تصـدر عن الاقتصـاد والإدارة ، المجلد ٢١ ،العدد ٢ ،٢٠٠٧م، ١٤٢٨ه، ص٥٣.

[461] (3741) الصـادر في ١٠ /نوفمبر ١٩٧٨م Stat. اذ ان قانون التحويل الإلكتروني الأمريكي رقم 95-630-92) الصـادر في ٢٢ مايو ٢٠٠٩م، وبالقانون رقم -111 (123 Stat. 1751)والمعدل بالقانون رقم (24؛-111 Stat. 2081 ،203؛ 124) ، والذي يعد من بين أول القوانين في الدول المتقدمة التى تنظم هذه العمليات، اذ اعتبر التحويل الإلكتروني في المادة (٧/٩٠٦) بأنه:"أي نقل للأموال (بخلاف الذي ينشأ باستخدام الشيكات أو الكمبيالات أو أي وسيلة ورقية مشابهة) يشرع به من خلال وحدة الإلكترونية أو أداه هاتفية أو حاسـب آلي أو أشـرطة مغناطيسـية، لأجل توجيه أمر أو تعليمات، أو الإذن التحويلات التي تتم عند نقاط - للمؤسسة المالية من أجل الإيداع أو السحب من الحساب. ويشمل- على سبيل المثال لا الحصر البيع، أو العمليات التي تتم بواسطة جهاز الصـراف الآلي، والتحويلات التي تتم من خلال استخدام الهاتف" للاطلاع على هذا "القـانـون مـن خـلال امـوقـع الالـكـتـرونـي الاتـي http://www.legifrance.gouv.fr/affichTexte.do?cidTexteJORFTEXT0 00026998473)

[462] د. بلال عبد المطلب بدوي ، مصدر سابق ، ص73 .

أمر دفع صادر عن بنك الآمر أو أي بنك وسيط يهدف إلى تنفيذ أمر الدفع الصادر عن الآمر [463]، و يلاحظ في التعريف السابق أنه لم يشترط كما فعل المشرع العراقي و المصري وجود حسابين للآمر و المستفيد وإنما اعتبر كل عملية يكون الهدف منها نقل مبلغ من النقود من الآمر إلى المستفيد هي عملية تحويل مصرفي .

يتضح مما سبق أن التوجهات الفقهية السابقة لم تركز على مضمون عمليات التحويل الإلكتروني، بقدر ما ركزت على الوسيلة المستخدمة في تنفيذها، بعكس التشريعات التي نظمت تلك العمليات والتي اهتمت بالوسيلة التي تستخدم في تنفيذها، وذلك بضرورة أن تكون من الوسائل الحديثة، بالإضافة إلى اهتمامها بمضمونها، حيث إن هذه الوظيفة في ظل تلك التشريعات لم تعد قاصرة على مجرد التحويلات من حساب إلى آخر، وانما توسعت بشكل كبير في مضمونها، بحيث تشمل كل ما من شأنه أن يؤثر على ذمة الزبون المالية، وهذا التوسع - من وجهة نظر الباحث- لا يستقيم مع طبيعة التحويل المالي كتقنية بنكية تتطلب تحويل النقود من حساب إلى حساب آخر.

وأن التحويل المالي الإلكتروني لا يختلف من حيث مضمونه عن التحويل المصرفي التقليدي، فهو " العملية التي يتم بمقتضاها تحويل مبلغ نقدي من حساب إلى حساب آخر باستخدام الأنظمة الإلكترونية، سواء كان الحسابان للزبون الآمر نفسه أو لشخصين مختلفين، وسواء تمت العملية فى المصرف ذاته أو اشترك فيها مصرفان فأكثر، وذلك بغض النظر عن الوسيلة التى استخدمها العميل في إرسال أمره للبنك، سواء كانت تقليدية أو إلكترونية. فالأنظمة الإلكترونية لم تغير من الطبيعة الذاتية للتحويل كتقنية يقوم بها المصرف، غير أن ذلك لا يعني أن تلك الوسائل الحديثة والمتطورة لم يكن لها تأثير على عمليات التحويل المصرفي الإلكتروني، فقد خلقت العديد من المشاكل المعقدة والخطيرة، حيث وسعت من التزامات أطراف عمليات التحويل بشكل كبير لم يكن معهوداً في ظل التحويلات التقليدية العادية، كما أنها أوجدت العديد من المخاطر التي قد تترتب عليها أضرار فادحة، سواء بالنسبة للزبون أو المصرف أو حتى المستفيد، والتي (أي الأنظمة الإلكترونية) أصبحت تنتج عنها مخاطر كبيره مع التطورات المتسارعة للأنظمة المعلوماتية، وما واكبها من تطور موازٍ أو قد يفوق عليها أحياناً في أساليب وطرق مجرمي وقراصنة تلك الأنظمة، بالإضافة إلى الصعوبات التي تواجه الزبائن في إثبات الأضرار التي قد تلحقهم نتيجة صعوبة حيازتهم لأدلة إثبات ما يدعونه، لاحتكار المصرف للوسائل والأنظمة التي تحتوي تلك الأدلة، وما نجم عن ذلك من صعوبة تحديد من المسؤول عن تلك الأضرار، خصوصاً في ظل القواعد العامة للمسؤولية المدنية التي قد لا تسعف في تحديد ذلك بما يتفق مع خصوصية هذه الأنظمة.

الفرع الثاني

مورد الخروج على الخصوصية في التحويل المالي الالكتروني

من خلال استقراء عقود الحسابات المصرفية وعقود استخدام أدوات التحويل المصرفي الإلكتروني المتاحة، فضلاً عن النصوص القانونية والتنظيمية ذات العلاقة بعمليات التحويل الإلكتروني، تبين لنا أن البنك يلتزم بالعديد من الالتزامات في مواجهة زبائنه سواء كانوا تجاراً ام أشخاصاً عاديين، ويمكن ان تكون بعض هذه الالتزامات محل خروج على حماية البيانات الشخصية للزبائن ، كالتزامه بالتأكد من سلامة المعاملة امنيا وذلك من خلال تزويد الجهات المختصة بمعلومات عن الزبون ، وأيضا حفظ بيانات الزبون الشخصية ،

---

[463] الدليل القانوني للتحويلات الإلكترونية للأموال، الذي أصدرته لجنة الأمم المتحدة للقانون التجاري الموحد UNCITRALسنة 1992 . متاح على الرابط الإلكتروني التالي :
http://www.uncitral.org/uncitral/ar/publications/publications.html

ولعل ابرزها هو الالتزام بالاعلام وهو ماسنتولى تعريفه أولا ، ومن ثم تحديد طبيعته ، وأخيرا المسؤولية المترتبة على عدم الالتزام به ، وكالاتي :

أولا : تعريف الالتزام بالاعلام : تقضي القواعد العامة في التعاقد بأن على كل من يقدم على التعاقد مع الغير أن يبحث بوسائله الشخصية عن المعلومات التي تلزمه لاتخاذ قراره في التعاقد[464] ، ولا تلزم الشركة المالية بناء على ذلك بتقديم أي معلومات؛ لأنه يجب على الشخص أن يتولى الدفاع عن مصالحه بنفسه، غير أن تطبيق هذه القواعد وإن كانت تنطلق من فكرة المساواة بين طرفي العقد لم تعد كافية لحكم العلاقة التعاقدية التي تجمع بين الشركة المالية بصفته طرفاً محترفاً والعميل أو المستهلك الذي يوصف بانه الطرف الضعيف بالعقد [465] . لذلك يكون هناك التزام على عاتق الشركة باعلام الزبون .

وعرف الالتزام بالاعلام بأنه "التزام أحد الطرفين بتقديم البيانات والمعلومات اللازمة لمساعدة الطرف الآخر على إبرام العقد أو تنفيذه، بل تحذيره ولفت نظرة إذا استدعي الأمر ذلك" [466].

وقد حاول البعض وضع تعريف مستقل للالتزام بالإعلام قبل التعاقد عن نظيره الخاص بمرحلة تنفيذ العقد[467]، ويعرف هؤلاء الالتزام الأول بأنه " التزام المهني السابق على التعاقد بتقديم المعلومات الجوهرية التي تفيد المستهلك، ولا يتمكن من الحصول عليها بوسائله الخاصة، نظراً لطبيعة العقد " أما الالتزام بالإعلام التعاقدي والخاص بمرحلة تنفيذ العقد فيعرف بأنه " التزام البائع بالإدلاء بالبيانات والمعلومات للمشتري بما يتفق مع موجبات حسن النية في التعامل والتي من شأنها أن تشكل رضا حرا ومستنيراً. "

وعلى أية حال فإن الغاية من الالتزام من الإعلام في صورتيه السابقة واللاحقة للتعاقد - كما ذكرنا– هي تنوير أرادة الزبون "المستهلك" وتبصيره بكافة المعلومات الجوهرية التي يجهلها، سواء من حيث نوعية خدمات التحويل التي تقدمها الشركة للزبون، والحدود المصرح بها إذا كانت قوانين الدولة تحدد مبلغ التحويلات بسقف معين، ومصاريف التحويل وغيرها من الالتزامات والواجبات التي يجب على الزبون القيام بها، في حالة التعاقد على فتح الحساب، أما في حالة التعاقد على تقديم أدوات إلكترونية للزبون لاستخدامها في إجراء التحويل عن بعد لا بد أن يشمل الإعلام على بيان أوصاف أداة التحويل، وخصائصها، وشروط العقد والتزامات أطرافه، وجزاء الإخلال بها، أو من حيث كيفية التعامل مع أداة التحويل محل التعاقد في مرحلة تنفيذ العقد بقصد الاستفادة القصوى منها، وتلافي الأضرار كافة التي يمكن أن تنجم في حالة استعمالها، أو عدم الاحتياط في حفظها، والتي يصعب على الزبون " المستهلك" الإحاطة بمضمون هذه المعلومات الجوهرية بدون مساعدة الطرف الأخر "الشركة " .

ثانيا : الأساس القانوني للالتزام بالاعلام : لقد أثار الأساس القانوني للالتزام بالإعلام جدلاً فقهيا واسع النطاق فظهرت العديد من الاتجاهات الفقهية التي تحاول وضع أساس قانوني له [468]. فهناك اتجاه يري أن الالتزام

---

[464] د. محمد مرسي زهرة، الحماية المدنية للتجارة الإلكترونية، (العقد الإلكتروني -الإثبات الإلكتروني – المستهلك الإلكتروني)، دار النهضة العربية، القاهرة ، ٢٠٠٨ ، ص١٧٠.

[465] هذه المساواة القانونية لا تستند - في كثير من الأحيان - إلى مساواة فعلية بين الطرفين، مما ينعكس في الغالب على مضمون العقد وشروطه وحقوق والتزامات كل من طرفيه لا سيما الطرف الضعيف فيه، فتزيد التزامات الأخير وسوء مركزه القانوني وهو ما يفيد منه الطرف القوي، الأمر الذي جعل المشرع والقضاء يتدخلان لمناصرة الطرف الضعيف، بمحاولة العدول عن فكرة المساواة القانونية لتحقيق فكرة المساواة الفعلية، وذلك بفرض القواعد التي تحمي الأخير من جور الطرف القوي وتسلطه . د/ محمد حسين عبد العال، مصدر سابق، ص16 .

[466] د. محمد المرسي زهرة ، مصدر سابق ، ص 173 .

[467] د. أشرف محمد مصطفى أبو حسين، التزامات البائع في التعاقد بوسائل الاتصال الحديث، منشأة المعارف، الإسكندرية، ٢٠٠٨ ، ص93

[468] د. حسام الدين كمال الأهواني، حماية المستهلك في إطار النظرية العامة للعقد، بحث مقدم إلى ندوة حماية المستهلك في الشريعة والقانون، التي نظمتها كلية الشريعة والقانون بجامعة الإمارات، في الفترة من ٦ -٧ ديسمبر، ١٩٩٨م، ص ٧.

بالإعلام يجد أساسه في القواعد الأخلاقية، والتي توجب هذه القواعد على المدين سواء في مرحلة ما قبل العقد أو في مرحلة تنفيذه عدم إخفاء معلومات جوهرية لا يمكن لمن تعاقد معه أن يصـــل إليها بعلمه الخاص، كما تقضي منه أن لا يقدم معلومات كاذبة وغير صحيحة [469].

ويؤكد أصحاب هذا التوجه أن القواعد الأخلاقية تعد ضرورة حتمية في حياة الأفراد في بناء الأنظمة القانونية التي تنظم شؤون حياتهم، فهي تعمل على إشاعة روح التعاون والتضامن فيما بينهم، وأن أية محاولة من قبلهم لهدم تلك القواعد الأخلاقية وتعطيل تطبيقها وإعمالها فيما بينهم، تنتهي بالفشـــل؛ لأنهم في نهاية المطاف يستسلمون لاحترامها ومراعاتها، فيضحي وجود الأخلاق فيهم وجود قهر وجبر لا وجود رغبة وقبول .

لهذا فإن كثيراً من الأحكام القانونية - وفقاً لهذا التوجه - ما هي إلا ترجمة لواجبات أخلاقية تم نقلها من المجال الأخلاقي إلى المجال القانوني، وبذلك فإن الضرورة الأخلاقية توجب حماية الشخص الضعيف من قوة تسلط الطرف الآخر وتعسفه في استخدام سلطته الاقتصادية . وينتقد البعض هذا التوجه على أساس أن هناك العديد من الالتزامات التي تســتند إلى أســس أخلاقية، إلا أنها في الواقع لا تحظى بالحماية القانونية اللازمة لإجبار الأفراد على تنفيذها واحترامها، لافتقارها إلى النصــوص القانونية التي تنظمها، وتفرض الجزاء المدني الذي يتلاءم مع حجم مخالفة المدين لها [470].

ويتجه آخرون إلى تأسيس الالتزام بالإعلام على أساس اقتصادي لتحليل الاعتبارات الداعية لمخالفة القاعدة العامة، والتي توجب على المتعاقد – في الأصل – أن يسعى بوسائله الخاصة نحو الاستعلام عما يتعاقد عليه، ويفرق أصــحاب هذا الاتجاه بين نوعين من المعلومات للقول بالاعتماد على الأســاس الاقتصــادي كأســاس للالتزام بالإعلام، أحدهما المعلومات المكتسبة بطريق القصد، أو العمد وهي التي يتحصل عليها المرء بتكلفة معينه وفي هذه يرون أنها لا تلزم المهني بالإعلام بالنسبة لها، وثانيها المعلومات المكتسبة بطريق المصادفة والتي حصل عليها بدون أي تكلفة وهي التي يلتزم المهني بالإعلام للزبون بها[471].

وعلى خلاف ذلك انتقد البعض هذا التوجه لعدم وجود حدود فاصلة وحاسمة بين نوعي المعلومات التي يقول بها أصحابه، ويرجع ذلك إلى أنه أعطى المعلومات المكتسبة بطريق القصد مدلولاً واسعاً إلى درجة كبيرة تجعله يشمل أي نوع من المعلومات، فيجعل وجود المعلومات المكتسبة بطريق المصادفة متلاشياً في الحقيقة والواقع وإن كان لها وجود من الناحية النظرية، بالإضـــافة إلى أنه ركز جل اهتمامه على الاعتبارات الاقتصـــادية فقط دون أن يراعي الاعتبارات الأخلاقية التي ترفض بكل إباء اســـتغلال المرء لجهل غيره، معتمداً في ذلك على ما لديه من معلومات فيستغلها لمصلحته ويخفيها عن غيره، ومع ما يترتب على ذلك من تغليب المصلحة الاقتصادية الفردية على المصلحة الاقتصادية العامة، والتي لا تتحقق إلا من خلال مراعاة الأفراد للمبادئ الأخلاقية التي تملي عليهم إبرام العقود على الصــدق والمكاشــفة بدلاً من الكتمان والمدالســة [472].

واتجه جانب من الفقه إلى إقامة الالتزام بالإعلام على أساس مبدأ حسن النية الذي يفرض على المتعاقد مراعاة الصدق والأمانة بما يحقق الثقة بين الطرفين، سواء قبل التعاقد أو بعده، ومن مقتضى ذلك أن يفصح المهني للزبون عند إبرام العقد كافة المواصفات والبيانات الضرورية عن الشيء محل التعاقد، والتي تجعل الزبون

---

[469] د. عبد الرحيم الشحات البحطيطي ، مصدر سابق ، ص56 .

[470] د. محمد أحمد عبد الحميد، الحماية المدنية للمستهلك التقليدي والإلكتروني ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠١٢م، ص 288.

[471] A.T. KRONMAN : Mistake, disclorue, information and the law of contrats ،Journal of legal studies 1978, p:I et S, cité par : MURIEL. Thèse précitée. N: 90, p:71.

نقلا عن الدكتور حسام الدين كامل الاهواني ، ، حماية المستهلك في إطار النظرية العامة للعقد ، مصدر سابق ، ص6 .

[472] د . خالد جمال أحمد، مصدر سابق، ص ٢٣٦

يقدم على التعاقد عن بينة من أمره، وأي كتمان لمثل هذه المعلومات يتنافى مع مبدأ حسن النية، بل قد يدل على سوء نية المتعاقد إذا كان يعلم أو يظن أن هذه البيانات لها تأثير على قرار المتعاقد الآخر بإبرام العقد أو الإحجام عنه، كذلك يقتضي هذا المبدأ أن يعلم الزبون بكافة المعلومات الجوهرية حول تنفيذ العقد [473].

وبذلك فإن الاعتماد على مبدأ حسن النية - وفقاً لهذا التوجه –لا يقتصر على مرحلة تنفيذ العقد، وإنما يمتد إلى مرحلة تكوين العقد من أجل تحقيق حماية الطرف الضعيف، والذي قد يكمن مصدر ضعفه في عدم العلم .

وانتقد البعض هذا الاتجاه على أساس أن الاعتماد على مبدأ حسن النية يكتنفه الكثير من الغموض، حيث يصعب في كثير من الحالات وضع مفهوم مستقر له، وبالتالي استنتاج التزامات قانونية محددة لتوفير حماية حقيقة للزبون[474]، ثم إن التشريعات نصت على هذا المبدأ في القسم المتعلق بآثار الالتزام في القانون المدني، بمعنى أنه يتعلق بمرحلة تنفيذ العقد، أي بعد أن يتم إبرام العقد، وبالتالي إذا كان يمكن اعتبار حسن النية أساساً للالتزام التعاقدي بالإعلام، فإنه من الصعب اعتباره أساساً للالتزام بالإعلام قبل التعاقدي، فهذا الأخير يهتم بتحسين رضا المستهلك بإعلامه قبل التعاقد حتى يقدم على التعاقد عن بينة واختيار.

ويرى اتجاه آخر أنه يستحيل تأسيس الالتزام بالإعلام على أساس واحد وأنه لا بد من تضافر مجموعة من الأسس تشكل في مجملها أساساً مشتركاً يرتكز عليه الالتزام بالإعلام، وتتمثل هذه الأسس - من وجهة نظره - في أساس أخلاقي واجتماعي وأساس اقتصادي وأساس قانوني، على اعتبار أن ما من واحد من هذه الأسس إلا وله بصمة قوية وأثر كبير في بناء وتدعيم قيام هذه الالتزام ونشأته في ميدان التعامل بين الاشخاص ؛ بحيث يصعب اعتبار أحد هذا الأسس الأساس الوحيد والفريد الذي يقوم على أكتافه الالتزام بالإعلام[475] .

وبذلك يرى الباحث أنه يمكن الاعتماد على "مبدأ حسن النية" في تنفيذ العقد كأساس لهذا الالتزام، والذي نص عليه القانون المدني ويوجب هذا المبدأ على المصرف أن يلتزم التزاماً إيجابيا بالصدق والأمانة[476]، بعدم إخلاله بالثقة التي وضعها فيه الزبون المتعاقد، ومن ثم يقع عليه تطبيقاً لهذا المبدأ الالتزام بمد الزبون بكل المعلومات اللازمة لمساعدته في الاستفادة من أداة التحويل الاستفادة الكاملة، وتحذيره من أية مخاطر تنجم عن استعمال تلك الأدوات استعمالاً خاطئاً أو غير مشروع.

ثالثا : محل الالتزام بالاعلام : ان محل الالتزام بالإعلام، سواء قبل التعاقد أو بعده، يشمل جميع المعلومات والبيانات الضرورية والجوهرية التي تهدف إلى تنوير إرادة العميل، وتساعده على استخدام أداة التحويل الاستخدام الأمثل بما يكفل تفادي أية مخاطر أو أضرار قد تلحقه من جراء إبرام العقد أو تنفيذه ، وقد حرصت التشريعات على بيان المعلومات التي يجب على المدين "الشركة" الالتزام بالإدلاء بها لصالح المستهلك الزبون، خصوصاً في المرحلة السابقة على التعاقد[477].

اذ يجب على المصرف عند قيامه بالتعاقد مع احد زبائنه، أن يقوم بالإدلاء بكافة المعلومات والبيانات المتعلقة بكافة الشروط التعاقدية التي تحكم التعامل في إحدى عمليات التحويل المالي الإلكتروني، بالشكل الذي يمكّن

---

[473] د. معتز نزيه محمد الصادق المهدي، الطبيعة القانونية لبطاقات الائتمان الإلكتروني المسئولية المدنية الناشئة عليها، دار النهضة العربية، القاهرة، ٢٠٠٦م، ص ٩٢ .

[474] د . خالد جمال أحمد، مصدر سابق، ص ٢٦٩.

[475] د . محمد أحمد عبد الحميد ، مصدر سابق ، 312 .

[476] نصت على هذا المبدأ المادة (١/١٤٨) مدني مصري، والتي جاء فيها " يجب تنفيذ العقد طبقاً لما اشتمل عليه، وبطريقه تتفق مع ما يوجبه حسن النية. "...

[477] Michel Jeantin ,Paul Le Cannu Thierry Granier,Richard Routier, Droit Commercial Instruments de paiement et de crédit titrisation, 8 ieme edition, Dalloz, 2010, p.215.

الزبون من الوقوف على مكونات هذا العقد وخصائصه الذاتية، ومدى جدواه وملاءمته في إشباع حاجته التي يرمي إليها؛ لما لذلك من أهمية بالغه في التأثير على قراره بالإقبال على التعاقد[478].

لذلك أوجبت العديد من التشريعات الخاصة بحماية المستهلك على المهني الالتزام بإحاطة المستهلك بكافة الشروط اللازمة للعقد المزمع أبرامه، وذلك من حيث مراحل التنفيذ، وما يرد بالعقد من ضمانات، وما إذا كانت هناك خدمة ما بعد التعاقد ستقدم للمستهلك من عدمه، كذلك مدة العقد، وتحديد مسؤولية المتعاقد، ومن ذلك ما نصت عليه المادة (L113-3) ، قانون الاستهلاك الفرنسي لسنة ١٩٩٣م، والتي أوجبت على كل مهني أن يعلم المستهلك بالظروف المتعلقة بعملية البيع أو الخدمة المطلوب تقديمها، والمسؤولية التعاقدية التي يتحملها المستهلك.

إلا أن المادة (L121-18) ، من القانون سالف الذكر والمضافة بموجب المرسوم رقم(٧٤١) لسنة ٢٠٠١ [479] ، كانت أكثر تفصيلاً في تحديد الشروط التي يلتزم المهني بإعلام المستهلك بها قبل التعاقد، حيث أوجبت عليه أن يحدد البيانات الخاصة به من حيث اسمه وعنوانه وأرقام تليفوناته، وطرق الدفع والتسليم والتنفيذ، والحق في الرجوع عن التعاقد، والمدة التي يظل الإيجاب ملزماً خلالها، ومدة العقد في العقود المستمرة أو الدورية[480].

ويتفق التوجيه الأوروبي رقم (97/7) EC / الخاص بالتعاقد عن بعد ، مع القانون سالف الذكر في هذا الشأن .

واستكمالاً لسياسة الحماية للمستهلك التي يتبعها المشرع الفرنسي، أصدر هذا المشرع قانون الثقة في الاقتصاد الرقمي رقم (٥٧٥) بتاريخ ٢٠٠٤ [481]، والذي تم بموجبه تعديل بعض أحكام مواد القانون المدني وقانون حماية المستهلك بما يجعلهما ملائمين لتنظيم العقود الإلكترونية وقد أولى هذا القانون اهتماماً خاص بالمستهلك الإلكتروني، حيث أوجبت المادة (١٩) والمادة (٢/٢٥) من هذا القانون على المهني في عقود الاستهلاك الإلكتروني، أن يتيح للمستهلك عبر الشبكة الشروط العامة للبيع، وذلك على نحو يسمح له بفهمها والاحتفاظ بها أو نسخها .

وقد حددت هذه المواد المعلومات التي يلتزم المهني بالإفصاح عنها للمستهلك الإلكتروني، وتتمثل في بيان الخطوات أو المراحل واجبة الاتباع لإبرام العقد الإلكتروني، مع بيان الوسائل التقنية التي تسمح للمستهلك بأن

---

[478] تجدر الإشارة هنا إلى أنه لا يتطلب من المدين المهني الالتزام بالإعلام بكل صغيرة وكبيرة من المعلومات التي يعرفها عن العقد المراد إبرامه، وإنما يقتصر التزامه بالإدلاء بالمعلومات الجوهرية التي تؤثر على قراره بشأن العقد وتفيده في تكوين رأيه عن محل العقد، والتي لا يستطيع الحصول عليها بوسائله الخاصة، وبالتالي فإنه لا يطالب المدين بإعلام دائنه بالمعلومات غير الجوهرية التي لا أثر لها على قرار الدائن بشأن العقد، كما أن الراغب في التعاقد لا يصدق عليه وصف "الدائن بالالتزام بالإعلام قبل التعاقد" متى أمكنه الوصول إلى المعلومات المتصلة بالعقد بوسائله الخاصة، أو كان عالماً بها من باب أولى، ولذلك فإنه يجب عليه الاستعلام عن المعلومات التي يمكنه التعرف عليها بطريقته الخاصة، كما عليه إن أراد مزيداً من المعلومات الثانوية المتصلة بالعقد، أن يبحث عنها بنفسه دون أن يكون له الحق في مطالبة غيره بها . د. خالد جمال أحمد، مصدر سابق، ص ٨٥، ٨٦ .

[479] وتقضي المادة (٩) من هذا القانون بأنه تستبدل المادة (L 121-18) بدل المادة (L 121- 18) من قانون الاستهلاك ومن غير المساس بالمعلومات المنصوص عليها في المادتين (L133-3) (L111-1) وكذلك المنصوص عليها في المادة-L.214 (1) حيث جاء فيها:

: Article 9 "L'article L. 121-18 du code de la consommation est remplacé par les dispositions suivantes Art. L. 121-18. - Sans préjudice des informations prévues par les articles L. 111-1 et L. 113-3 ainsi que de celles prévues pour l'application de l'article L. 214-1…".

[480] راجع نصوص قانون الاستهلاك الفرنسي وفق النسخة الموحدة رقم ٧٣٧-٢٠١٠م الصادر في ٢٠١٠/٧/١م على الرابط الإلكتروني?http://www.legifrance.gouv.fr/affichCode.do :

[481] متاح هذا القانون على الرابط الالكتروني الاتي :
http://www.legifrance.gouv.fr/affichTexte.do?cidTexteJORFTEXT00 0000801164

يتعرف عليها قبل إبرام العقد على البيانات التي ينوى التوقيع عليها وما يشوبها من أخطاء، وقدرته على تصحيحها، بالإضافة إلى ما يقترحه المهني من لغات لإبرام العقد، وشروط الدخول للعقد المخزن والمحفوظ لدى الموجب المهني، والوسائل التي يلتزم المستهلك بإتباعها للتعرف إلكترونياً على القواعد المهنية والتجارية التي يخضع لها المهني عند اللزوم[482].

ونظرا لأهمية العقود الالكترونية ومنها عقد التحويل المالي قامت العديد من التشريعات التي نظمت عمليات التحويل المصرفي الإلكتروني للأموال بالنص على التزام خاص بالإعلام، يوجه إلى كل شخص ينوي التعاقد مع المصرف بخصوص إحدى عمليات التحويل المالي الإلكتروني، ويلتزم المصرف بموجب هذا الإعلام الخاص، بالإفصاح بكل البيانات والمعلومات التي حددتها نصوص هذه التشريعات، بالشكل الذي يضمن أن يكون هذا الإعلام واضحاً وصادقاً وكاملاً يعكس علماً حقيقيا بمضمون العقد، بحيث يستطيع الزبون على ضوئه أن يقْدم على التعاقد مع البنك في ظل رضا حر مستنير، وهو عالم بحقيقة ما يقدم عليه.

وقد حدد المشرع الفرنسي في المادة (L314-12) من قانون النقد والمالية [483] البيانات التي يلتزم المصرف أن يعلم الزبون بها قبل إبرام عقد تقديم خدمات الدفع، حيث نص على ضرورة أن تتضمن تلك البيانات جميع الشروط المتعلقة بتقديم الخدمة، وكذلك كافة البيانات المتعلقة بمقدم خدمة الدفع، بالإضافة إلى الشروط المتعلقة بإنهاء وتعديل العقد.

وبخصوص وقت الإدلاء بتلك المعلومات، فكونها تتعلق بالشروط اللازمة للتعاقد، فالمنطق يقتضي أن يتم الإفصاح عنها في المرحلة السابقة على إبرام العقد، ولا يتصور أن يحقق هذا الالتزام غايته والحكمة من وجوده، إلا إذا تم تنفيذه قبل إبرام العقد بفترة زمنيه كافية، وهذا ما نصت عليه المادة الرابعة من التوجيه الأوروبي والخاص بحماية المستهلك في التعاقد عن بعد كما تولت بيان التوقيت الذي يجب تنفيذ الالتزام بالإعلام خلاله المادة (L111-1) من قانون الاستهلاك الفرنسي، والتي أوجبت أن يتم ذلك قبل إبرام العقد بوقت مناسب.

وبخصوص الوسيلة التي يجب أن يتم فيها هذا الإعلام، فقد اشترط كل من المشرعين الفرنسي في الفقرة الأولى من المادة (L314-13) من قانون النقد والمالية ، أن يكون الإعلام بواسطة وثيقة مكتوبة أو أى وسيلة أخرى موثوق بها، وأن تكون واضحة ومفهومة بسهولة .

ويمكن للمصرف أن يوفي بهذا الالتزام وفقاً للشكل المطلوب إذا ما قام بتسليم نسخة من مشروع العقد للزبون[484]، حتى يتسنى له الاطلاع عليه وتفحصه وقراءته أكثر من مرة بسهولة ويسر، ليس فقط بالاعتماد على توضيحات المصرف، بل كذلك بأخذ المشورة ممن يثق به وله إلمام بالعملية حتى يكون تعاقده عن تبصر وعلم كافيين ، وتكمن أهمية هذه الوسيلة في أنها تعمل على محاربة بعض الممارسات من طرف المهنيين

---

[482] ينتقد البعض هذا القانون على أساس أنه أغفل ذكر بعض البيانات التي قد تمثل أهمية كبيره للمستهلك، كشروط التسليم والاستبدال، ومدى وجود خدمة الصيانة، أو خدمة ما بعد البيع، وإمكانية الرجوع في التعاقد من عدمه. انظر د. محمد أحمد عبد الحميد ، مصدر سابق ، 326 .

[483] قام المشرع الفرنسي بالنص على التزام البنك بإعلام العميل في المادة (L314 - 12) التي أحالت على الفقرة الثانية من المادة (L314 13) والتي تضمنت المعلومات التي يجب على البنك إعلام الزبون بها، حيث جاء النص كالآتي : "....les informations et les conditions sur le prestataire de services de paiement ،sur l'utilisation d'un service de paiement ،sur les frais ،les taux d'intérêt et les taux de change ،sur Ia surlacommunication entre l'utilisateur et le prestataire de services de paiement ،sur les mesures de protection et lesmesures correctives ،sur la modification et la résiliation du contrat-cadre et sur les recours ...."

[484] اشترط المشرع الفرنسي في الإعلام عن طريق العقد، أن يتم بناء على طلب العميل وذلك في المادة (L314- 13) من قانون النقد والمالية، وتطلب أن يتضمن هذا العقد، جميع المعلومات الواردة في المادة (L314- 12) والسابق الإشارة إليها.

الذين قد لا يقبلون تسـليم الوثائق التعاقدية إلا بعد التوقيع على العقد بالشـكل الذي يحرم المسـتهلك من كل إمكانية لدراسة العقد قبل إبرامه[485] .

وأيضـا الى جانب ما سبق اعتمدت اغلب المؤسسـات المصـرفية مؤخرا نظام جديد للتحويلات البنكية معتمدا على ال IBAN وهو رقم الحساب المصرفي الدولي وهو الرقم الخاص بالزبون المعترف به من قبل البنوك والمؤسسـات المالية في جميع انحاء العالم وهو طريقة قياسـية لتحديد الحسـاب المصـرفي ، وهو ما يقلل من الأخطاء والتأخير في ارسـال المدفوعات المحلية والدولية ، وهو يتكون من بيانات تخص الزبون وكود للبنك المصدر، ويعد بمثابة تعريف للشخص في النظام البنكي المحلي والدولي . وهو ما يعد من البيانات الشخصية الخاضعة للحماية [486] .

وبالرغم من اعتبار المحكمة الاوربية لحقوق الانسان البيانات المستنتجة من المعطيات المصرفية بيانات ذات طابع شخصـي سواء اعتبرت بيانات حساسة ام لا [487] . وعرجت المحكمة على انه قد تتعلق هذه المعلومات أيضـا بالمعاملات المهنية وليس هناك سـبب مبدئي لتبرير اسـتبعاد الأنشـطة ذات الطبيعة المهنية او التجارية من مفهوم الحياة الخاصة .

وعلى الرغم من ذلك فان الإعلان عنها للطرف الاخر في عملية التحويل لا يشكل انتهاك للبيانات الشخصية ، كون ان طبيعة العملية يتطلب العلم بهذه البيانات لضرورتها وهذا لا يشكل تدخل في حياة الزبون الخاصة ، مما يعفي المؤسـسـة المصـرفي من الملاحقة القانونية على الرغم من اطلاع الغير على هذه البيانات وهو ما يشكل قيد على المسؤولية القانونية ومنع تطبيق احكامها .

---

[485] لا شك أن إعلام الزبون عن طريق العقد وسيلة فعالة إذا ما قورنت بالإعلان، فهذه الأخيرة وسيلة لجذب المستهلك تقدم في صـورة معلومات توجه إلى الجمهور دون أن تحمل كافة التفاصـيل الدقيقة عن الخدمة أو المنتج، فالإعلان لا يكون صـادقاً بالمعنى الدقيق، لأن الأوصـاف التي يحملها وأن كانت صـادقة في ذاتها، فهي لا تحمل إلا جانباً من جوانب المنتج أو الخدمة، ويترك الجانب الذي يحمل تنبيهات قد تصـرف الزبون عنها، بينما الإعلام عن طريق العقد يهدف إلى حماية الزبون بتقديم معلومات موضـوعية وصـادقة عن المنتج أو الخدمة محل التعاقد. للمزيد من الاطلاع انظر :الدكتور عبد الحميد الدياسطي عبد الحميد، آليات حماية المستهلك في ضـوء القواعد القانونية لمسـئولية المنتج" دراسـة مقارنة"، دار الفكر والقانون، المنصـورة طبعة ٢٠٠٩م ، ص١٩٧.

[486] د. اية لبيب محمد عبد الرحمن ، الحماية القانونية للهوية الرقمية ، دار النهضة العربية ، ط1 ، 2023 ، ص 134 .

[487] CASS CEDH , 7 Juillet 2015 , m , n c/ Saint – Marin , req . n. 28005/12 , p . 51 .

الخاتمة

ان توفير الحماية القانونية للبيانات الشخصية مطلب تنشده روح العدالة والفطرة السليمة للانسان ، بيد ان توفير هذه الحماية مرهون بسن تشريعات تستجيب لمتطلبات العصر ، ومن هنا كانت اهمية اختيارنا لموضوع هذه الاطروحة ، والذي رصدنا من خلالها خطورة غياب التنظيم القانوني لهذه الحماية ز
ومن ثم فقد توصلنا الى جملة من النتائج والتوصيات وكالاتي :

اولا : النتائج : توصلت الدراسة الى عدة نتائج هي :

1- **على الرغم من تعدد التشريعات الوطنية والدولية المنظمة لموضوع الدراسة (حماية البيانات الشخصية) الا انها قد اجتمعت جميعها عند هدف واحد يرمي الى تقرير حماية تلك البيانات ومنع الاعتداء عليها .**
2- **ان القوانين المقارنة والمنظمة لحماية الحق المذكور قد قصرت تطبيقه على البيانات المتعلقة بالاشخاص الطبيعية والمعالجة الكترونيا بشكل كلي او جزئي دون امتداد نطاقه الى معالجة البيانات المكتوبة او المخزونة ورقيا بصورة كاملة او المتعلقة بالاشخاص المعنوية .**
3- توسع المشرع الأوروبي في تحديد نطاق تطبيق اللائحة الإقليمي مستهدفا كل شركة تقوم بمعالجة بيانات شخصية تتعلق بمواطن أو مقيم في إحدى دول الاتحاد ولو لم تكن الشركة قد تأسست في إحدى دول الاتحاد وليس لها مقر أو فرع فيها، وحتى لو لم يكن البلد العضو هو مركز النشاط الفعلي لها، مما يعد خروجا على المعايير التقليدية المتعارف في تحديد نطاق تطبيق التشريعات، وهو أمر محمود فرضته في تقدير الباحث طبيعة شبكة الإنترنت التي تسمح بالتعامل مع البيانات عن بعد.
4- اختلفت تحديدات التشريعات المقارنة لاسيما اللائحة الأوروبية والقانون المصري لمضمون البيانات الحساسة، فالمشرع الأوروبي يشير إلى البيانات التي تفصح عن الأصل العرقي أو الاثني أو العضوية النقابية والبيانات المتعلقة بالطبيعة أو الحياة الجنسية وهي بيانات لم يشر إليها المشرع

المصـري. ومن جانب آخر يشـير المشـرع المصـري إلى بيانات الحالة الأمنية وهو مالم تشـر إليه اللائحة الأوروبية.

5- أجمعت التشـريعات المقارنة المنظمة لحماية البيانات الشـخصـية على الزام الشـركات المالية القائمة بجمع بيـانـات الزبـائن ومعـالجتهـا ببيـان الغرض من الجمع والمعـالجـة ، بحيث لا يجوز اســتخدام المعلومات والبيانات المسجلة لديها في غير الاغراض التي جمعت من اجلها .

6- قننـت اغلـب التشـريعات المقارنـة عـدة حقـوق لصـاحب البيانـات الشخصـية حقـه فـي الاطـلاع عليهـا وتصـحيحها ، وحقـه فـي الاعتـراض علـى معالجتهـا ، وحقـه فـي سـحب موافقتـه المسـبقة علـى معالجـة بياناتـه الشخصـية الـى غيـر ذلـك مـن الحقـوق ، وفـي ذات الوقـت الزمـت التشـريعات ذاتهـا الشـركة بمجموعـة مـن الالتزامـات منهـا علـى سـبيل المثـال ، الالتـزام بمعالجـة البيانـات بأمانـة ومشـروعية ، والمحافظـة علـى سـلامة وسـرية البيانـات ، واتخـاذ الاحتياطـات اللازمة لحماية البيانات ، وايضا حذف او محو البيانات .

7- يترتـب علـى الاعتـداء علـى البيانـات الشخصـية ، ان مـن حـق المعتـدى علـى بيانتـه ان يطلـب وقف الاعتداء كما له الحق كذلك في طلب التعويض .

8- لا يشـكل افشـاء البيانـات الشخصـية فـي بعـض الاحيـان فعـل تعـدي بسـبب سـماح المشـرع بـذلك ، امـا لكـون طبيعـة المعاملـة تقتضـي الافصـاح عـن بيانـات الزبـائن الشخصـية ، او لضـرورات امنية .

ثانيا : المقترحات :

1- دعـوة المشـرع العراقـي نحـو الاسـراع الـى سـن تشـريع يعنـى بحمايـة البيانـات الشخصـية ، علـى ان يراعـي عنـد اعـداد مشـروعه مراجعـة نصـوص التشـريعات المقارنـة لا سـيما اللائحـة الاوربيـة رقـم (679) لسـنة 2016 ، وذلـك بغيـة الاحاطـة باحكامهـا علـى ان يتضـمن هـذا التشـريع القواعـد الخاصـة بمشـروعية التعامـل مـع البيانـات الشخصـية ، خاصـة فيمـا يتعلـق ببيـان غرضـها ، وفئـات البيانـات الشخصـية ، ونطـاق القيـود المفروضـة ، والضـمانات الراميـة الـى منـع اسـاءة المعاملـة او الوصـول غيـر القـانوني الـى البيانـات او نقلهـا بصـورة غيـر مشـروعة مـع تحديـد جهـة او هيـأة مختصـة تعنـى بحمايـة تلـك البيانـات وممارسـة الرقابـة علـى الأشـخاص الـذين يحصـلون عليهـا مـن خـلال تعـاملاتهم مع زبائنهم.

2- دعـوة البنـك المركـزي العراقـي علـى متابعـة حمايـة البيانـات الشخصـية لحـين تـدخل المشـرع بوضـع تشـريع خـاص يسـتهدف تحديـد نطاقهـا واليـة حمايتهـا دون الاكتفـاء بـبعض النصـوص المتنـاثرة فـي قـوانين عـدة ، والقيـام باتخـاذ الاجـراءات المناسـبة والكفيلـة لحمايـة البيانـات ، بمـا يمنـع الاعتـداء عليهـا ، والـذي يمكـن ان ينـتج عـن جمعهـا ومعالجتهـا والتصـرف بهـا ،ومخاطبـة كافـة الجهـات المعنيـة بالعمـل علـى رصـد انشـطة كافـة الشـركات والجهـات التـي تقـوم بجمـع البيانـات او تقـوم ببيعهـا لاخـرين لاغـراض تجاريـة ربحيـة او تسـويقية بطريقـة غيـر مشـروعة ، تمهيـدا لاتخـاذ الاجـراءات القانونيـة بحقهم .

3- الـى ان يضـع المشـرع العراقـي هـذا القـانون فانـه يجـب علـى القضـاء ان يقـوم بـدوره الرئيسـي فـي حمايـة هـذه البيانـات عـن طريـق اعمـال قواعـد المسـؤولية التقصـيرية وذلـك بتكييـف فعـل الاعتـداء علـى بيانـات الزبـائن الشخصـية بأنهـا خطـأ تقصـيري ، ومـن ثـم يـتم تعـويض صـاحبها عمـا لحقـه مـن ضـرر بسبب التعدي عليها .

4- دعـوة المشـرع العراقـي الـى التوسـع فـي تحديـد نطـاق تطبيـق التشـريع العراقـي المـأمول علـى غـرار اللائحـة الأوربيـة نظـرا للطبيعـة العالميـة لنشـاط أبـرز الشـركات المتعاملـة مـع البيانـات الشخصـية علـى شبكة الانترنت.

5- دعـوة البنـك المركـزي العراقـي الـى ضـرورة التنسـيق علـى كـل مـن المسـتويين المحلـي والـدولي بمـا يـؤمن الانسـجام بـين قـوانين الحمايـة ويضـمن التـدفق الحـر للبيانـات بـين الحـدود فـي اطـار مـن الحماية .

6- دعـوة البنـك المركـزي العراقـي ضـرورة تعزيـز الشـفافية وارسـاء قواعـد الحوكمـة الرشـيدة فـي مجال نشر وتبادل البيانات ، في اطار من الحفاظ على الخصوصية وسرية البيانات .

7- يجب على البنك المركزي العراقي نشر ثقافة قانونية وتقنية تهدف الى تعريف وتوعية الافراد بالمخاطر التي تحيط ببياناتهم الشخصية المفصح عنها الى الشركات المالية عند التعامل معها والية حمايتها سواء ببنود العقد المبرم مع تلك الشركات او من خلال التبصير بنصوص القانون الحامية لها .

المصادر

القسم الأول: المصادر العربية:

- القرآن الكريم.

أولًا: معاجم اللغة العربية:

1- ابن منظور، لسان العرب، الجزء ١١، الطبعة الأولى، دار صادر، بيروت، من دون ذكر سنة النشر.

2- ابن منظور، لسان العرب، ج ٤، دار صادر للطباعة والنشر، دار بيروت للطباعة والنشر، بيروت، ١٩٥٦م

3- احمد بن فارس بن زكريا القزويني الرازي ، معجم مقياس اللغة ، تحقيق عبد السلام محمد هارون ، دار الفكر ، 1979 .

4- الفيروز آبادي، القاموس المحيط، ج (٤) دار العلم للجميع، بيروت.
5- مجمع اللغة العربية، معجم القانون، الهيئة العامة لشؤون المطابع الأميرية، القاهرة، ١٩٩٩.
6- محمد بن ابي بكر بن عبد القادر الرازي ، مختار الصحاح ، دار الكتب الحديثة ، الجزء الاول ، 1978.

ثانيًا: الكتب القانونية:

1- د. احمد رجب سيد صميدة ، التنظيم القانوني للحق في الخصوصية ، (المسكن ، الاتصالات الخاصة ، البيانات الشخصية) ، ط1، دار النهضة العربية ، القاهرة، 2022 .
2- د. احمد شوقي عبد الرحمن ، مسئولية المتبوع باعتباره حارسا ، دار الفكر العربي ، القاهرة ، 1998.
3- د. احمد محمود سعد ، استقراء لقواعد المسؤولية المدنية في منازعات التلوث البيئي، ط1 ، دار النهضة العربية ، ط1 ، القاهرة ، 1994 .
4- د. اسامة عبد الخالق الانصاري ، ادارة البنوك التجارية والبنوك الاسلامية ، المكتبة العربية للنشر والتوزيع ، 1994 .
5- د. اسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دار النهضة العربية ، القاهرة ، 1994 .
6- د. أسامة عبد المنعم علي إبراهيم، حصر ومكافحة غسيل الاموال ومكافحة تمويل الارهاب والنقل غير المشروع للاموال عبر الحدود في التشريعات العربية، المركز القومي للاصدارات القانونية، الطبعة الاولى، 2009 .
7- د. أشرف محمد مصطفى أبو حسين، التزامات البائع في التعاقد بوسائل الاتصال الحديث، منشأة المعارف، الإسكندرية، ٢٠٠٨ .
8- د. العربي جنان ، معالجة المعطيات ذات الطابع الشخصي ، الحماية القانونية في التشريع المغربي والمقارن ، ط1، المطبعة الوطنية ، مراكش ، 2010 .
9- اياد محسن ضمد ، حماية حق الخصوصية من تأثير الاعلام في العراق ، مكتبة صباح ، بغداد ، 2017.
10- د. اية لبيب محمد عبد الرحمن ، الحماية القانونية للهوية الرقمية ، دار النهضة العربية ، ط1 ، 2023 .
11- د. باسم محمد فاضل مدبولي ، المسؤولية المدنية عن اضرار معالجة البيانات الرقمية ، دار الفكر الجامعي ، ط1 ، 2020 .
12- د. بهاء المري ، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الاثبات ، ط1، العربية للنشر والتوزيع ، 2018 .
13- د. توبي مندل و اندو بوديفات واخرون ، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير ، منشورات اليونسكو ، سلسلة اليونسكو لحرية الانترنت ، 2012 .
14- د. جميل الشرقاوي ، النظرية العامة للالتزام ، الكتاب الأول ، مصادر الالتزام ،دار النهضة العربية ، القاهرة ، 1995 .
15- د. حسام الدين كامل الاهواني ، الحق في احترام الحياة الخاصة ، دار النهضة العربية ، القاهرة ، 1978.
16- د. حسن جميعي ، مسئولية المنتج عن الاضرار التي تسببها منتجاته المعيبة ، دار النهضة العربية ، القاهرة ، 2000 .
17- د. حسن علي الذنون ، النظرية العامة للالتزامات (مصادر واحكام الالتزام) المكتبة القانونية ، بغداد ، 1976 .
18- د. حسن محمد احمد حسن ، محتوى الحسابات الرقمية ومدى انتقاله للغير ، دار الوفاء ، الإسكندرية ، ط1 ، 2022 .
19- د. حسن محمد ثاني، سيكولوجية الارهاب، مكتبة عالم الكتب، القاهرة، 2006 .
20- د. خالد حسن احمد ، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية ، دار الكتب والدراسات العربية ، 2020 .

21- د. خالد حسن احمد ، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية ، دار الكتب والدراسات العربية ، ط1، 2020 .
22- د. خالد سري صيام، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالثقة العامة وجرائم الارهاب وتمويله، الطبعة1، 2006م.
23- د. خالد ممدوح ابراهيم ، الجريمة الالكترونية ، الدار الجامعية ، ط 1 ، 2008 .
24- د. خالد ممدوح إبراهيم ، امن الجريمة الالكترونية ، ط1 ، الدار الجامعية ، الإسكندرية ، 2008 .
25- د. خليف مصطفى ، الحماية القانونية للحق في الحياة الخاصة ، ط1 ، مكتبة الوفاء القانونية ، مصر ، الاسكندرية ، 2021.
26- د. دياب سليمان ، اقتصاديات النقود و البنوك ، المؤسسة الجامعية للدراسات والنشر والتوزيع ، 1996.
27- د. رضا السيد عبد الحميد، النظام المصرفي وعمليات البنوك، دار النهضة العربية، القاهرة، ٢٠٠٨.
28- د. رضوان اسخيطة ، اضاءة على اللائحة العامة الاوربية لحماية البيانات الشخصية ، 2018
29- د. سارة الشريف ، خصوصية البيانات الرقمية ، الاصدار الثالث ، سلسلة اوراق الحق بالمعرفة ، مركز دعم لتقنية المعلومات ، القاهرة ، 2014.
30- د. سارة علي رمال ، الحق في الخصوصية في العصر الرقمي ، منشورات الحلبي الحقوقية ، 2018.
31- د. سعد غالب التكريتي، بشير عباس العلاف، الأعمال الإلكترونية، دار المناهج، الأردن، بدون تاريخ نشر
32- د. سعيد حسب الله عبد الله ، شرح قانون أصول المحاكمات الجزائية ، دار الحكمة ، الموصل ، 1990.
33- د. سليم عبد الله الجبوري ، الحماية القانونية لمعلومات شبكة الانترنت ، منشورات الحلبي الحقوقية ، ط1، 2011 .
34- د. سليمان مرقس ، الوافي في شرح القانون المدني ، الفعل الضار ، الجزء الثالث
35- د. سمير حسني المصري ، المسؤولية التقصيرية الناشئة عن استخدام الانترنت ، دار النهضة العربية ، ط1، القاهرة ، 2017.
36- د. سهير منتصر ، النظرية العامة للحق ، منشورات جامعة الزقازيق ، مصر ، 2006 .
37- د. سيد اشرف جابر ، مسؤولية مقدمي خدمات الانترنت عن المضمون الالكتروني غير المشروع ، دار النهضة العربية ، القاهرة ، 2010 .
38- د. شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لحق الإطلاع على البيانات الشخصية- دراسة مقارنة،دار الفكر والقانون ، الطبعة الأولى، المنصورة،2015 .
39- د. شوقي يعيش تمام ، الجريمة المعلوماتية ، مطبعة الرمال ، الجزائر ، 2019 .
40- د. طارق جمعة السيد راشد ، المسؤولية التقصيرية للناشر الالكتروني عن انتهاك الحقوق المالية للمؤلف ، دار النهضة العربية ، 2012 .
41- د. طالب جواد عباس ، د. عبد الجبار ضاحي عواد ، الدليل الرقمي واثره في الاثبات ، زين الحقوقية ، بيروت ، 2016 .
42- د. عبد الحميد الدياسطي عبد الحميد، آليات حماية المستهلك في ضوء القواعد القانونية لمسئولية المنتج" دراسة مقارنة"، دار الفكر والقانون، المنصورة طبعة ٢٠٠٩م .
43- د. عبد الرحمن خليفة الرواس ، اثر التشريعات المتعلقة بحماية البيانات الشخصية على فعالية التجارة الالكترونية ، منشورات زين الحقوقية ، ط1 ، 2019 .
44- د. عبد الرحمن خليفة الرواس ،اثر التشريعات المتعلقة بحماية البيانات الشخصية على فعالية التجارة الالكترونية ، زين الحقوقية ، ط1 ، 2019.
45- د. عبد الرزاق احمد السنهوري ، الوسيط في المسئولية المدنية ، الجزء الأول ، الفقرة 571 .
46- د. عبد الفتاح عايد فايد ، التعويض التلقائي للاضرار بواسطة التأمين وصناديق الضمان ، دار الجامعة الجديدة ، الاسكندرية ، 2014 .
47- د. عبد المنعم السيد علي ، النقود والمصارف والاسواق المالية ، دار الحامد للنشر ، ط1 ، 2004.

48- د. عبد الهادي فوزي العوضي ، الحق في الدخول في طي النسيان على شبكة الانترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 2013 .
49- د. عبد الهادي فوزي العوضي ، الحق في الدخول في طي النسيان على شبكة الانترنت ، دار النهضة العربية ، ط1 ، 2014.
50- د. عبد الهادي فوزي العوضي ، المسؤولية التقصيرية لناشري برامج التبادل غير المشروع للمصنفات الفكرية ، دار النهضة العربية ، القاهرة ، 2016 .
51- د. علاء فرحان طالب والدكتور حيدر يونس كاظم والدكتور محمد فائز حسن ، مدخل في ادارة المؤسسات المالية ، مركز كربلاء للدراسات والبحوث ، ط1 ، 2016 .
52- د. علي محمد جواد عطا ، رقابة البنك المركزي العراقي على المؤسسات المالية الخاصة ، دار امجد للنشر والتوزيع ، عمان ، 2019 .
53- د. عمار عباس الحسيني ، جرائم الحاسوب والانترنت ، الجرائم المعلوماتية ، منشورات زين الحقوقية ، ط1 ، بيروت ، لبنان ، 2017 .
54- د. عمار عباس الحسيني ، جريمة الاتلاف المعلوماتي ، دراسة قانونية مقارنة ، منشورات زين الحقوقية ، ط1، بيروت ، لبنان ، 2019.
55- د. عمر احمد حسبو ، حماية الحريات في مواجهة نظم المعلومات ، دار النهضة العربية ، القاهرة ، 2000 .
56- د. عمرو طه بدوي ، التنظيم القانوني لمعالجة البيانات الشخصية ، ط1، دار النهضة العربية ، القاهرة ، 2020 .
57- د. فهمي مصطفى الشيخ ، التحليل المالي ، Sme Financinl ، ط1 ، 2008 .
58- د. فؤاد الشعيبي ، التنظيم القانوني لعقود خدمات الاتصالات ، منشورات الحلبي الحقوقية ، ط1، 2014.
59- د. لطيف جبر كوماني ، الوجيز في شرح قانون الشركات الاردني ، دار الابجدية للنشر والتوزيع ، عمان ، 1994 .
60- د. محمد اتلشوا ، ثورة المعلومات وانعكاسها على قانون العقوبات ، دار النهضة العربية ، ط2، القاهرة ، 2000 .
61- د. محمد أحمد عبد الحميد، الحماية المدنية للمستهلك التقليدي والإلكتروني ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠١٢.
62- د. محمد السيد عرفة، الاتفاقية الدولية لقمع تمويل الارهاب ومدى فاعليتها في مكافحته، دراسة تأصيلية تحليلية مقارنة، جامعة نايف العربية للعلوم الامنية، الرياض، 2013 .
63- د. محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠٠٩.
64- د. محمد الشهاوي ، الحماية الجنائية لحرمة الحياة الخاصة ، دار النهضة العربية ، القاهرة ، 2005 .
65- د. محمد حسن قاسم ، المدخل لدراسة القانون – القاعدة القانونية ، نظرية الحق ، ج2 ، منشورات الحلبي الحقوقية ، بيروت ، 2009 .
66- د. محمد حسين منصور ، نظرية الحق ، دار الجامعة الجديدة ، الاسكندرية ، 1998 .
67- د. محمد سامي عبد الصادق ، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية ، دار النهضة العربية ، 2016 .
68- د. محمد سعيد عبد الله الحميدي، المسؤولية المدنية الناشئة عن تلوث البيئة البحرية والطرق القانونية لحمايتها وفقا لقانون دولة الامارات العربية المتحدة ، دار الجامعة الجديدة ، ط1 ، الاسكندرية ، 2008 .
69- د. محمد عمر ذوابة، عقد التحويل المصرفي الإلكتروني، دار الثقافة للطباعة والنشر، الأردن، ٢٠٠٦.
70- د. محمد مختار مختار فودة ، قانون التجار الدولي في المعاملات الالكتروني ، دار النهضة العربية ، 2022 .

71- د. محمد مرسي زهرة، الحماية المدنية للتجارة الإلكترونية، (العقد الإلكتروني -الإثبات الإلكتروني – المستهلك الإلكتروني)، دار النهضة العربية، ٢٠٠٨ .
72- د. محمد مؤنس محب الدين، الارهاب في القانون الجنائي على المستويين الوطني والدولي، دار النهضة العربية، القاهرة، 1998 .
73- د. محمود أبو فروة ، مسؤولية البنك المدنية في عمليات التحويل الالكتروني، دار وائل للطباعة والنشر والتوزيع، الأردن، عمان، ٢٠١٤.
74- د. محمود رجب فتح الله ، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري رقم 175 لسنة 2018 ، دار الجامعة الجديدة ، الإسكندرية ، 2019 .
75- د. مصطفى الجمال ود. رمضان ابو السعود ، د. نبيل ابراهيم سعد ، مصادر واحكام الالتزام ، منشورات الحلبي ، 2003 .
76- د. مصطفى العوجي ، القانون الجنائي العام ، ج2 ، المسؤولية الجنائية ، بيروت ، 1985 .
77- د. معتز نزيه محمد الصادق المهدي، الطبيعة القانونية لبطاقات الائتمان الإلكتروني المسئولية المدنية الناشئة عليها، دار النهضة العربية، القاهرة، ٢٠٠٦م.
78- د. ممدوح خليل بحر ، حماية الحياة الخاصة في القانون الجنائي ، دار النهضة العربية ، القاهرة ، 1983.
79- د. منتصر سعيد حمود، الارهاب الدولي، جوانبه القانونية، ووسائل مكافحته في القانون الدولي العام والفقه الاسلامي، دار الفكر الجامعي، الاسكندرية، الطبعة الاولى، 2008 .
80- د. منصور بن صالح السلمي ، المسئولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي ، جامعة نايف للعلوم الأمنية ، الرياض ، 2010 .
81- د. منى الأشقر جبور ، د. محمود الجبور ، البيانات الشخصية والقوانين العربية ، الهم الأمني وحقوق الافراد ، المركز العربي للبحوث القانونية والقضائية ، ط1، بيروت ، 2018 .
82- د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الاقتصادية ، دار النهضة العربية ، القاهرة ، 2004 .
83- د. نبيل محمد عثمان عرعارة ، الحماية الجنائية للحق في حرمة المراسلات عبر البريد الالكتروني ، المصرية للنشر والتوزيع ، ط1 ، 2018 .
84- د. نسرين محسن نعمة الحسيني و الدكتور محمد حسن مرعي ، الجرائم الالكترونية الواقعة على الاموال ، المكتب الجامعي الحديث ، مصر ، 2020 .
85- د. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، 2008 .
86- د. هيام الجرد ، المد والجزر بين السرية المصرفية وتبييض الاموال ، منشورات الحلبي الحقوقية ، ط1، 2004 .
87- د. هيثم السيد احمد عيسى ، التشخيص الرقمي لحالة الانسان في عصر التنقيب في البيانات عبر تقنية الذكاء الاصطناعي ، وفقا للائحة الاوربية العامة لحماية البيانات لعام 2016 ، دار النهضة العربية ، 2019 .
88- د. وسيم شفيق الحجار ، النظام القانوني لوسائل التواصل الاجتماعي ، المركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية ، ط1 ، بيروت ، 2017 .
89- د. وسيم شفيق الحجار ، النظام القانوني لوسائل التواصل الاجتماعي ، (واتساب ، فيسبوك ، تويتر) ، ط1 ، المركز العربي للبحوث القانونية ، بيروت ، 2017 .
90- د. وفاء حلمي ، محاضرات في نظرية الحق ، منشورات جامعة الزقازيق ، مصر ، 2007 .
91- د. وليد السيد سليم، ضمانات الخصوصية في الانترنت، دار الجامعة الجديدة، 2012 .

ثالثًا: الرسائل والاطاريح الجامعية

1- د. اسماء حسن سيد محمد رويعي ، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية ، أطروحة دكتوراه مقدمة الى كلية الحقوق / جامعة القاهرة ، 2013.
2- د. اية لبيب محمد عبده عبد الرحمن ، الحماية القانونية للهوية الرقمية ، أطروحة دكتوراه مقدمة الى كلية الحقوق جامعة عين شمس ، 2022 .

3- د. جوهر زايد جوهر المهندي ، الحماية الجنائية لحرمة الحياة الخاصة في القانون القطري " دراسة مقارنة " اطروحة دكتوراه مقدمة الى كلية الحقوق جامعة القاهرة ، 2019.
4- حنين جميل أبو حسين ، الاطار القانوني لخدمات الامن السيبراني ، رسالة ماجستير مقدمة الى كلية الحقوق ، جامعة الشرق الأوسط ، المملكة الأردنية الهاشمية ،2021 .
5- د. خالد جمال حامد عبد الشافي، المواجهة التشريعية لظاهرة الارهاب، دراسة مقارنة، اطروحة دكتوراه مقدمة الى كلية الحقوق جامعة عين شمس ،2015.
6- د. راجي عبد الملك، دراسة شرعية وقانونية لوسائل ونظم الدفع الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهره، ٢٠١٠.
7- د. عبد الرحمن جمال الدين حمزة، الحق في الخصوصية في مواجهة حرية الإعلام ، اطروحة دكتوراه، كلية الحقوق، جامعة المنوفية، 2002 .
8- د. عبد المجيد كوزي ، الحماية القانونية للبيانات والمعطيات ذات الطابع الشخصي ، أطروحة دكتوراه مقدمة الى كلية العلوم القانونية والاقتصادية والاجتماعية ، جامعة سيدي محمد بن عبد الله ، فاس ، 2015 .
9- د. عثمان بكر عثمان ، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي ، اطروحة دكتوراه ، جامعة طنطا ، 2020 .
10- د. علاء عيد طه ، الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها ، أطروحة دكتوراه مقدمة الى كلية الشرق العربي للدراسات العليا في الرياض ، 2018 .
11- د. كريم محمد محي الدين سليم ، نطاق الحق في الخصوصية ومدى تأثره بالتقنيات الحديثة ، اطروحة دكتوراه مقدمة الى كلية الحقوق جامعة المنوفية ، 2018 .
12- د. ماشاء الله عثمان محمد الزوي ، الحماية الجنائية لحرمة الحياة الخاصة في التشريع الليبي بالمقارنة مع التشريعين الفرنسي والمصري ، أطروحة دكتوراه مقدمة الى كلية الحقوق / جامعة القاهرة ، 2012.
13- د. محمد علي العريان ، الجرائم المعلوماتية ، اطروحة دكتوراه ، كلية الحقوق ، جامعة الاسكندرية ، 2011.
14- د. محمود محمد لطفي محمود صالح ، أطروحة دكتوراه مقدمة الى كلية الحقوق جامعة طنطا ، 2009 .
15- د. محمود محمد محمد ابراهيم فياض ، المسؤولية المدنية الناشئة عن استخدام تكنولوجيا الاعلام والاتصال ، اطروحة دكتوراه مقدمة الى جامعة المنصورة – كلية الحقوق ، 2018 .
16- د. مروة زين العابدين صالح ، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت ، اطروحة دكتوراه ، جامعة عين شمس ، 2016 .
17- د. يحيى صقر أحمد صقر، حماية حقوق الشخصية في إطار المسؤولية التقصيرية، دراسة مقارنة ، اطروحة دكتوراه ، كلية الحقوق - جامعة القاهرة ، 2006.

رابعًا: البحوث والمقالات القانونية:

1- د. احمد عرف احمد يوسف ، الاعتداء على الحياة الخاصة في مواقع التواصل الاجتماعي ، بحث منشور في مؤتمر الضوابط القانونية والاخلاقية للاعلام، كلية الحقوق – جامعة عين شمس ، 2018.
2- د. احمد فتحي سرور ، الحق في الحياة الخاصة ، بحث منشور في مجلة القانون والاقتصاد ، مطبعة جامعة القاهرة ، العدد 54 ، 1986 .
3- احمد هادي كعود ، الحق في الخصوصية والجرائم الواقعة عليها ، بحث مقدم الى المعهد القضائي العراقي ، 2013 .
4- د. اسامة غانم العبيدي ، التفتيش عن الدليل الرقمي في الجرائم المعلوماتية ، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب ، جامعة نايف العربية للعلوم الأمنية ،المجلد 29 ، 2013 ، العدد 58 .

5- د. الصالحين محمد العيش، تعليق حول حكم محكمة العدل الأوروبية الصادر في 13 مايو 2014 بشأن الحق في اعتبار بعض الوقائع في طي النسيان، بحث منشور بمجلة معهد دبي القضائى، العدد 5، 3 فبراير 2015 .
6- د. الياس أبو جودة: الإرهاب والجهود الدولية والإقليمية لمكافحته، مجلة الجيش، لبنان، العدد (91) كانون الثاني ٢٠١٥.
7- امام حسانين خليل، جرائم تمويل الارهاب في التشريع المصري، بحث مقدم إلى المؤتمر الرابع عشر للجمعية المصرية للقانون الجنائي حول تحديات العولمة والعدالة الجنائية، القاهرة، في الفترة من 19 إلى 20 مايو، القاهرة، 2009 .
8- د. جبالي ابو هشيمة كامل ، حماية البيانات الشخصية في البيئة الرقمية ، بحث مقدم الى مؤتمر العصر الرقمي واشكالياته القانونية ، كلية الحقوق ، جامعة اسيوط ، من 12-13 ابريل 2016 .
9- د. حسام الدين كمال الأهواني، حماية المستهلك في إطار النظرية العامة للعقد، بحث مقدم إلى ندوة حماية المستهلك في الشريعة والقانون، التي نظمتها كلية الشريعة والقانون بجامعة الإمارات، في الفترة من ٦ -٧ ديسمبر، ١٩٩٨.
10- حسام محمد نبيل الشنراقي، حماية البيانات الشخصية عبر الانترنت التحديات والحلول، المجلة العربية للادارة، ملحق العدد الثاني، المجلد 38 ،2018 .
11- د. دعاء حامد محمد عبد الرحمن ، احكام العلاقة بين مقدمي خدمة الانترنت والمستخدمين بشأن انتهاك حقوق الملكية الفكرية ، مجلة الحقوق للبحوث القانونية والاقتصادية ، العدد الثالث ، 2018.
12- د. زكريا يونس احمد ، اثبات عملية التحويل المصرفي الالكتروني وحجيتها ، مجلة جامعة تكريت للحقوق ، السنة السادسة ، المجلد السادس ، العدد (2)الجزء (2) 2022 .
13- د. سالم علي الظنحاني، الإطار القانوني لمكافحة تمويل الإرهاب «دراسة قانونية سياسية»، مجلة الشرق الأوسط، مركز بحوث الشرق الأوسط بجامعة عين شمس، مصر، عدد (33) سبتمبر ٢٠١٣م.
14- د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات الشخصية ، القسم الاول ، بحث منشور في مجلة الحقوق الكويتية ، العدد 3 ، 2011.
15- د. سامح عبد الواحد التهامي ، الحماية القانونية للبيانات للشخصية ، القسم الثاني ، مجلة الحقوق الكويتية ، العدد 4 ، 2011 .
16- د. سامح عبد الواحد التهامي ، ضوابط معالجة البيانات الشخصية ، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي ، مجلة كلية القانون الكويتية ، العدد 9 ، السنة الثالثة ، 2015 .
17- د. سامح عبد الواحد التهامي ، نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها ، مجلة البحوث القانونية والاقتصادية ، الامارات العربية ، العدد 67 ، 2018 .
18- د. سامية عبد الرزاق خلف ، التعدي على حرمة الحياة الخاصة باستخدام التكنولوجية الحديثة ، مجلة الدراسات القانونية ، العدد 25 ، 2010 .
19- د. شريف يوسف خاطر ، حق الاطلاع على البيانات الشخصية في فرنسا ، مجلية كلية الحقوق الكويتية العالمية ، العدد 9 ، السنة الثالثة ، 2015 .
20- د. شريف يوسف خاطر ، حماية الحق في الخصوصية المعلوماتية ، مجلة البحوث القانونية والاقتصادية ، جامعة المنصورة ، العدد 57 ، 2015 .
21- د. صبري حمد خاطر ، تطور فكرة المسؤولية التقصيرية ، بحث منشور في مجلة دراسات قانونية ، العدد الأول ، السنة الثالثة ، بيت الحكمة ، بغداد ، 2001 .
22- د. صفاء حسن نصيف ، التحديات الإجرائية المتصلة بالجرائم المعلوماتية ، بحث منشور في مجلة العلوم القانونية والسياسية ، جامعة بغداد ، المجلد الخامس ، العدد الثاني ، 2016 .
23- د. طارق جمعة السيد ، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي ، بحث منشور في مجلة القانون والاقتصاد المصرية ، ملحق العدد 94 ، 2021 .
24- د. عبد الرحيم الشحات البحطيطي، المخاطر المالية في نظم المدفوعات في التجارة الإلكترونية كأحد التحديات التي تواجه النظم المصرفية، مجلة جامعة الملك عبد العزيز، الاقتصاد والإدارة ، المجلد ٢١ ،العدد ٢ ،٢٠٠٧.

25- د. علي حامد علي الخولي ، مكافحة تمويل الإرهاب ، بحث منشور في مجلة الحقوق جامعة الإسكندرية المجلد 1 ، العدد 4 السنة 2018 .
26- د. فضل يوسف إدريس، جريمة تمويل الإرهاب في القانون السوداني، مجلة جامعة بحري للآداب والعلوم الإنسانية، السنة الخامسة، ع: (9) أغسطس ٢٠١٦.
27- د. ما شاء الله عثمان الزوي، الحماية الجنائية للبيانات الشخصية الالكترونية في القانون الليبي والمقارن، مجلة العلوم الشرعية والقانونية، كلية القانون بالخمس، جامعة المرقب، العدد الأول ، 2018 .
28- د. محمد احمد المعداوي ، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي ، بحث منشور في مجلة كلية الحقوق جامعة بنها ، العدد 33 ، الجزء الرابع ، 2016 .
29- د. محمد بن فردية ، الدليل الجنائي الرقمي وحجيته امام القضاء الجنائي ، بحث منشور في المجلة الاكاديمية للبحث القانوني ، كلية الحقوق والعلوم السياسية جامعة بجاية ، السنة الخامسة ، المجلد 9 ، العدد 1 ، 2014 .
30- د. محمد محمد القطب مسعد ، الحماية المدنية للمعلومات الشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال والتواصل ، بحث منشور في مجلة البحوث القانونية والاقتصادية ، كلية الحقوق جامعة المنصورة ، العدد 67 ، 2018 .
31- د. محمود وهيب ، ظاهرة العولمة وانعكاساتها الأمنية ، بحث منشور في المجلة العربية لعلوم الشرطة ، مطابع الشرطة ، القاهرة ، العدد 164 ، 1999.
32- د. معاذ سليمان الما، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الإلكترونية الحديثة دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس، 9 - 10 مايو 2018 ، ملحق خاص، العدد 3، الجزء الأول، مايو 2018 .
33- د. معاذ سليمان الملا ، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الالكترونية الحديثة _ دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي _ بحث منشور في مجلة القانون الكويتية العالمية ، العدد 33، الجزء الأول ، 2018 .
34- د. معاذ سليمان الملا ، فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الالكترونية الحديثة ، مجلة كلية القانون الكويتية العالمية ، العدد الثالث ، 2018 .
35- د. منى تركي و د. جان سيريل فضل الله ، الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة ، مجلة كلية بغداد للعلوم الاقتصادية الجامعة ، العدد الخاص بمؤتمرها ، 2013 .
36- د. منى عبد العالي موسى ، مصطفى كريم هادي ، وسائل اثبات جريمة الازعاج بواسطة الوسائل السلكية واللاسلكية ، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية ، المجلد 26، العدد 9، 2018.
37- د. ميسون خلف حمد الحمداني ، مشروعية الأدلة الالكترونية في الاثبات ، بحث منشور في مجلة كلية الحقوق جامعة النهرين ، العدد 2 ، المجلد 18 ، 2016 .
38- د. هايدي عيسى ، الحاجة لمظلة تشريعية لمارد الدفع الرقمي ، الحاضر والمستقبل ، مجلة جامعة الشارقة للعلوم القانونية ، المجلد 17 ، 2020 .
39- د. هشام عمر أحمد الشافعي، التعاون الدولي لمنع تمويل الإرهاب، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، مجلد (٢٥)العدد: (٩٧) ،أبريل ٢٠١٦ .
40- د. يوسف بن أحمد الرميح، تمويل الارهاب، طرق ملتوية وأساليب قد تخفي على البعض، جريدة الاقتصادية أون لاين 2007 على الموقع الاتي: http://www.aleqt.com.

خامسًا: التشريعات:

1- القانون المدني العراقي رقم 40 لسنة 1951 .
2- قانون التجارة العراقي رقم 30 لسنة 1984 .
3- قانون الشركات العراقي رقم (21) لسنة 1997 المعدل .
4- قانون المصارف العراقي رقم 94 لسنة 2004 .

5- قانون اصول المحاكمات الجزائية العراقي رقم 17 لسنة 2008.
6- قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم (78) لسنة 2012 .
7- قانون مكافحة غسيل الاموال وتمويل الإرهاب العراقي رقم (39) لسنة 2015 .
8- الدليل الارشـــادي الخاص بمؤشـــرات الاشـــتباه في عمليات غســـل الأموال وتمويل الإرهاب المتعلقة بالمعاملات المصرفية لسنة 2017 والصادر من البنك المركزي العراقي.
9- دليل العمل الرقابي الصادر من البنك المركزي العراقي بالكتاب رقم 136/2/9 في 2019/4/1 .
10- القانون المدني المصري رقم (131) لسنة 1948 .
11- القانـون رقـم 61 لسـنة 1963 بشـأن إصـدار قانـون الهيئـات العامـة.
12- قانون توظيف الاموال المصري رقم 146 لسنة 1988
13- قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004 .
14- قانون حماية البيانات الشخصية التونسي رقم 63 لسنة 2004 .
15- قانون حماية الاشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي المغربي لعام 2009.
16- قانون المعاملات الالكترونية الكويتي رقم 20 لسنة 2014 .
17- قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.
18- قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 .

القسم الثاني: المصادر الأجنبية:

أولا: الكتب القانونية:

1- Celine Castets-Renard , Droit de I Internet : Droit francais et europeen , 2eme edition , Montchrestien , L,extensor editions , 2012 .
2- Cristina Cotaneu , the cyberconsumer, protection ,on, line at data of being on line is , 2001.
3- Geoffrey Turk; money and currency in the 21 st Century, July 1997.
4- Goldman (B.), La determination du garden responsible du fait des choses inanimees, these, Lyon, 1945.
5- Michel Jeantin ,Paul Le Cannu Thierry Granier,Richard Routier, Droit Commercial Instruments de paiement et de crédit titrisation, 8 ieme edition, Dalloz, 2010.
6- Patrice Jourdain, Genevieve Viney : Traite de droit Civil , Les conditions de la responsabilite Dommage, fait generateur , regimes speciaux , causalite , 4e edition , Editeur:L.G.D.J , 2013 .
7- Rowenna Fielding, 'The Concept of Controller and Processor Data Entities' 2018.
8- Suzanne Carval , Patrice Jourdain , Genevieve Viney : Les effets de Ia responsabilite 4e edition , Editeur : L . G . D . J , 2017 .

ثانيًا: البحوث والمقالات القانونية:

1- Alexandare Menais and Sophie des Courits , High standards apply to personal data processing .
2- Clair Laybats and John Davies, 'GDPR: Implementing the Regulation' (2018) 35(2) Business Information Review.
3- Elizabeth Holland Capel 17 Elizabeth Holland Capel , Conflict and Solution in Delawar,s Fiduciary Access to Digital Assets and Digital Accounts Act , Volume

30 , Issue 4 Annual Review the Law Journals and Related Materials at Berkeley Law , 2015.

4- Janos Meszaros, 'Two Different Approaches of the Data Protection Law: the European Union and the United State' (2015) 9(1) Journal of Legal and political Sciences 1, 12
5- Lauren Moius & Nathalie Krup International Joumal of Communication 3 (2009).
6- Lauren Movius and Nathalie Krup, 'US and EU Privacy policy: Comparison of regulatory Approaches' (2009) International Journal of Communication.
7- Linda Maizener , member du consell d,administration de I,Association des jeunes magistrats Tout Ie dommage , rien que Ie dommage ? Gaz , pal . 24 juill . 2018 , n GPL329s3.
8- Lothar Deterinann , Social Media Privacy : A Dozen Myths and Facts , 2012 STANFORD Technology Law Review .
9- Mark Phillips, 'International Data-Sharing Norms: from the OECD to the General Data Protection Regulation (GDPR)' (2018) 137(8) Human Genetics.
10- Michelle Goddard, 'The EU general Data Protection Regulation (GDPR): European Regulation That has a Global Impact' (2017) 59(6) International Journal of Market Research 703, 705
11- Mpakwana Annastacia Mthembu, Electronic Funds Transfer: Exploring the Difficulties of Security, Journal of International Commercial Law and Technology Vol. 5, Issue 4 (2010).
12- Nadezhda Purtova (2018), the law of everything Broad concept of personal data and future of Eudata protection law, Innovation and technology,10:1,40-81, Dol :1001080,17579961020180145217 6
13- Nadezhda Puytova , Tocite this article ; Nadezhda(2018) The law of every thing . Broad concept of personal data and Future of E U data Protection law ,Innovation and Technology , 10:1 , 40 -81,dol: 10-1080\17579961, 2018 .
14- Nathalie Mallet . Poujol ,Protectionde lavie priree et desdonnres , Personnelles, etude disponible enlign a al adresse:https :\\eduscot , education fy\ Chrgt \ guideVie Privee . pif , le :18\3\2020.
15- Paul Lambert , DATA Protection, DATA Loss and Penalties , (2012)4 IBLQ 22.
16- Reidenberg , J,R .(2000) Resolving conflicting international data privacy rules in cyberspace.stanford law Review,52,1315-1371.
17- Rikke Jorgensen, 'Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google' (2017) 35(2) Nordic Journal of Human Rights
18- Sabine Lipovetsky et Audry Yayon-Dauvet, Le devenir de la protection des données personnelles sur internet, Gaz. pal, 12,13 septembre 2001, 121?? année, nQ 255 à 256.

19- Sulliman Omarjee , Le data mining : Aspects juridiques de I,intelligence artificielle au regard de la protection des donnees personnelles , memoire , faculte de droit , universite montpellier I, Annee universitaire 2001-2002.

ثالثًا: التشريعات:

1- قانون شركات الاستثمار الفرنسي الصادر عام 1945 والمعدل في 1957 .
2- قانون المعلوماتية والحريات الفرنسي رقم (78) لسنة 1978 والمعدل.
3- قانون العقوبات الفرنسي ذي العدد 653 لسنة 1994 .
4- اللائحة الاوربية لحماية البيانات الشخصية رقم 46 لسنة 1995 الملغاة .
5- قانون حماية البيانات الشخصية الفرنسي لسنة 1978 والمعدل عام 2004 .
6- قانون معالجة البيانات الشخصية لدولة جزر الفارو رقم 429 لسنة 2011.
7- اللائحة الاوربية لحماية البيانات الشخصية (GDPR) لسنة 2016 .

رابعًا: المواقع الالكترونية:

1- http://www.legifrance.gouv.fr
2- https://www.ftc.gov/system/files/documents/cases/d09389-comm-final-orderpublic.pdf}
3- http:// canlaw : findlanv : com/ us – lst – circuit / 1663921.html
4- http://www.legifrance.gouv.fr/affichCode.do
5- http://www.uncitral.org/uncitral/ar/publications/publications.html
6- www.droit-technologie.org
7- http // curia.europa.eu/juris/liste.jsf?num=C-101/01
8- http :\\www.loc.gov\law\foreign-news\article\germany-federal-court-of-jusice-rules-digital-social-media-accounts-inheritable.
9- http://lita-Ib.org/archive/56-questions-answers-html
10- http://web.archive. org/ web/ 20010410032230
11- http://www.avocats-mathias.com/wp-personnel-Janvier-2017,pdf.
12- http://www.bqilii.org
13- http://www.comunc.como.it/il
14- http://www.euractiv.com.
15- http://www.legifrance.gouv.fr/affichTexte.do?cidTexteJORFTEXT00 0000801164
16- http:/www. goldmoney. com/ futuremoney. html.
17- https//:iapp.org/news/a/german-dpas-push-model-for-higher-gdpr-fines/-
18- https//:transparencyreport.google.com/euprivacy/overview?hl=ar&hl=es
19- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/
20- https://www.7iber.com/society/facebook-cyber-crimes.
21- www . dalloz . fr
22- www . juriscom . net
23- www .Iegifrance.gouv.fr
24- www.Legi France .gouv-Fr .
25- www/droitntic.com

Abstract

Personal data and information hold significant economic value in the context of corporate business transactions at the present time. Companies generally seek to collect, process, and exchange individual data in order to enhance their profits and economic benefits. Companies, such as those providing educational and medical services, social media platforms, or financial institutions like banks, primarily rely on dealing with individuals' personal data at both national and international levels. However, this activity can have negative effects on individuals' privacy and personal lives, as well as on the economic and social systems of countries."

On this basis, many legislative institutions, whether international or local, attempted to regulate the transmission and flow of information in a way that guarantees the intended economic benefits and preserves, in turn, the rights of individuals and their personal lives. However, an organization of this kind was surrounded by difficulties due to the absence of international regulation first, and the nature of dealing with data and its transmission, which often extends to more than one country, which requires. Subjection to different legal regulations.

As the different legal systems and their philosophies related to human rights, security and even commercial dimensions require legal regulation that crosses the borders of local jurisdictions to ensure the protection of this data and ensure that it is not infringed upon.

For this reason, these legislations imposed legal obligations on companies dealing with this data, and granted rights to their owners, And in the event of infringement or non-compliance with these obligations and failure to guarantee rights, companies bear legal responsibility, Except in some cases in which the law

permitted the possibility of disclosure, whether due to the nature of the transaction or for security reasons.

Republic of Iraq

Ministry of Higher education and scientific research

University of Babylon

College of Law

The Legal Protection of Personal Data for Customers of Financial Companies

A Comparative Study

A dissertation submitted by the student (Alkarar Habeeb Jahlool) to the Council of the college of Law University of Babylon

It is part of the requirements for the degree of Doctor of Philosophy in Private Law

Supervised by

Prof. Mithaq Talib Abd Hammadi Al-Jubouri

Professor of commercial law