



جامعة آل البيت

كلية الدراسات الفقهية والقانونية

قسم الدراسات القانونية

الحماية الجزائية للمعلومات الشخصية للأفراد  
في مواجهة أخطار بنوك المعلومات  
"دراسة مقارنة"

The Punitive Protection Of The Individuals Personal Information In Facing The  
Dangers Of Data Banke

(A Comparative Study)

إعداد الطالب:

محمد رشيد حامد ابو حجيله

الرقم الجامعي: (٠٢٢٠٢٠٠٠٠١)

إشراف الدكتور:

محمد نواف الفواعره

قدمت هذه الرسالة إستكمالاً لمتطلبات الحصول على درجة الماجستير في القانون في كلية الدراسات الفقهية والقانونية  
في جامعة آل البيت

٢٠٠٧



جامعة آل البيت

كلية الدراسات الفقهية والقانونية

قسم الدراسات القانونية

الحماية الجزائية للمعلومات الشخصية للأفراد  
في مواجهة أخطار بنوك المعلومات  
"دراسة مقارنة"

The Punitive Protection Of The Individuals Personal Information In Facing The  
Dangers Of Data Banke  
(A Comparative Study)

إعداد الطالب:

محمد رشيد حامد ابو حجيلة

الرقم الجامعي: (٠٢٢٠٢٠٠٠٠١)

التوقيع

أعضاء لجنة المناقشة:

الدكتور محمد نواف الفواعره..... مشرفاً ورئيساً

الأستاذ الدكتور سلطان عبد القادر الشاوي..... عضواً

الدكتور معتصم خميس مشعشع..... عضواً

الدكتور سامر محمود الدالعة..... عضواً

قدمت هذه الرسالة إستكمالاً لمتطلبات الحصول على درجة الماجستير في القانون في كلية الدراسات الفقهية والقانونية  
في جامعة آل البيت

نوقشت وأوصي بإجازتها بتاريخ / ٢٠٠٧

باكورة  
عملي العلمي  
إلى

والذي الحبيب أطال الله في عمره  
والدتي الحنونة التي أعطت بلا حدود أطال الله في  
عمرها

أخواني وأخواتي الأعزاء حفظهم الله

زوجتي وأبنائي البراعم البرئية

"باسل وبتول ودعاء وبنان"

حفظهم الله جميعاً

كل إنسان محب للعلم والعلماء

الحمد لله رب العالمين والصلاة والسلام على المبعوث رحمةً للعالمين النبي العربي الهاشمي الأمين وعلى آله وصحبه وسلم بإحسان إلى يوم الدين .

وبعد .....

بادئ ذي بدء فإنني أتوجه إلى جامعتي الحبيبة ، جامعة آل البيت ممثلةً برئيسها وأعضاء الهيئتين التدريسية والإدارية بجزيل الشكر وعظيم الإمتنان لما قدمته من تعاون في سبيل إنجاز هذا البحث العلمي الذي يضيف لبنة جديدة من لبنات العلم والمعرفة الى مكتبتنا العربية.

كما أتوجه بجزيل الشكر والتقدير والإحترام إلى أساتذتي الأفاضل ، أعضاء لجنة المناقشة والحكم على الرسالة ، فأتوجه بجزيل الشكر إلى أستاذي الفاضل الدكتور محمد الفواعرة المشرف على الرسالة لما أبداه من أراء سديدة وتوجيهات قيمة طيلة فترة إشرافه على الرسالة .

كما أتوجه بجزيل الشكر والتقدير إلى إستاذنا الكبير الدكتور سلطان الأشاوي رئيس جامعة بغداد سابقاً ، ورئيس قسم القانون الجزائي في جامعة عمان العربية لما أبداه من ملاحظات قيمة أثناء مناقشته الرسالة .

أما أستاذنا الدكتور معتصم مشعشع فله منا كل الحب والإحترام حيث أدني تتلمذت على يديه اثناء دراستي في جامعة آل البيت . أما الدكتور سامر الدالعة فله الشكر والإحترام لما أبداه من ملاحظات قيمة وأراء سديدة أثناء مناقشته الرسالة .

كما لا يسعني في هذا المقام إلا أن أتوجه بجزيل الشكر والتقدير والإحترام إلى إختنا الفاضلة أم فؤاد التي سهرت الليالي في طباعة هذه الرسالة وإنجازها على هذا الشكل .

أما الزملاء في مديرية التربية والتعليم لواء قسبة المفرق فلهم مني كل الإحترام والتقدير، وأخص بالذكر الزملاء في قسم الرقابة والتفتيش .

## Contents

٣	إهداء
٤	الشكر
٥	قائمة المحتويات
٦	الملخص
٨	مقدمة
٨	موضوع الدراسة :-
١٢	أهمية الدراسة :
١٤	مشكلة الدراسة :
١٥	عناصر المشكلة :
١٥	أهداف الدراسة :
١٦	التعريف بالمصطلحات :
٢٠	منهج الدراسة :
٢٠	خطة الدراسة :
٢١	تقسيم الخطة:
٢٢	الفصل الأول
٢٣	مخاطر بنوك المعلومات على حق الفرد
٢٣	في خصوصية معلوماته
٢٧	المبحث الأول
٣٨	المبحث الثاني
٧١	الفصل الثاني
٧١	تمهيد وتقسيم :-
٧٤	المبحث الأول
٩١	المبحث الثاني
١٢٣	الخاتمة
١٢٩	نتائج الدراسة
١٣١	التوصيات
١٣٣	قائمة المصادر والمراجع

تناولت هذه الدراسة موضوع الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات وهو من المواضيع التي لم تتناوله التشريعات إلا حديثاً ، رغم أن حق الفرد في خصوصية معلوماته له ارتباط وثيق بمسألة غاية في الأهمية والخطورة في حياة الفرد وهي حرّيته ، على اعتبار أن حق الانسان في الخصوصية يشكل جوهر الحقوق والحريات الشخصية .

حاولت هذه الدراسة إمكانية التعرف إلى مدى الحماية التي أضفاها قانون العقوبات الأردني على حق الفرد في الخصوصية لضمان احترامه في ظل التطورات العلمية الحديثة ، بالإضافة إلى بيان المخاطر التي تتعرض لها المعلومات الشخصية نتيجة للثورة العلمية الهائلة في تقنيات الأجهزة الحديثة ، خاصة بنوك المعلومات والتي أدى ظهورها إلى تهديد أسرار الحياة الخاصة للأفراد إذ أنه يضع تحت تصرف الدولة وأجهزة الأمن والمشروعات العامة والخاصة حجماً كبيراً من المعلومات عن خصوصية الفرد تعجز الوسائل العادية أو الأساليب التقليدية عن الوصول إليها الأمر الذي يستدعي وجود تنظيم قانوني لحماية البيانات والمعلومات الشخصية من مخاطر هذه البنوك .

ومن الجدير بالذكر أن بنوك المعلومات قد لعبت دوراً كبيراً في تقدم المجتمع الحديث الذي اصبح يعتمد على المعلومات باعتبارها عصب الحياة الاقتصادية والسياسية والإجتماعية ، إلا أن هذه البنوك قد شكلت خطراً داهماً على حق الفرد في خصوصية معلوماته ، حيث ساهمت في تقييد الحقوق والحريات الشخصية للأفراد عن طريق جمع وترتيب وتخزين ومعالجة المعلومات الإسمية المتعلقة بهم ، هذا الخطر يتمثل في السماح بجمع البيانات عن الأشخاص مع عدم معرفة أوجه استخدامها في المستقبل ، حيث أنها قد تستخدم في غير الغرض المخصص لها ، أو استخدامها في غير ما يلائم صاحبها أو يوافق صاحب الشأن أو دون رضاه ، بالإضافة إلى جمع بيانات عن شخص دون سبب مشروع ، مما يعد انتهاكاً للحياة الخاصة وتهديداً للحريات الفردية ، الأمر الذي حدا

ببعض الدول أن تصدر التشريعات الملزمة من أجل حماية البيانات الأسمية من أخطار بنوك المعلومات .

وتجدر الإشارة هنا أن هذه الدراسة ، هدفت إلى مراعاة التوازن بين مصلحة الفرد في صون أسرار حياته الخاصة والحفاظ قدر الإمكان على معلوماته الشخصية من أخطار بنوك المعلومات ، وبين مصلحة المجتمع في المساس بهذه الأسرار وكشفها في بعض الحالات الموجبة لذلك .

وقد تبين أنه نتيجة لتضافر جهود الفقه والقضاء والقانون المقارن في كل من فرنسا وأمريكا وألمانيا ، فقد تم الإتفاق على وضع مجموعة من المبادئ والضمانات والتي تهدف إلى وضع الفرد في موقع متقدم في مواجهة تلك الإعتداءات لكي يتمكن من السيطرة على معلوماته بإعتبار أن الخصوصية التي تدور حول الحماية هي خصوصية المعلومات كما أن من شأن هذه المبادئ والضمانات أن تقلل من مخاطر الإعتداء على البيانات الخاصة للأفراد إذا ما تم الأخذ بها والعمل على إبرازها في التشريعات العادية .

لقد تبين أن هناك عدداً من التشريعات التزمت الصمت نحو أخطار بنوك المعلومات على البيانات الشخصية للأفراد وهي غالبية تشريعات الدول النامية، ومنها التشريع الأردني ، حيث إكتفى بالنصوص الخاصة بحماية الأسرار .

وخلصت هذه الدراسة إلى عدة توصيات منها :-

أولاً :- إيجاد تشريع خاص لحماية البيانات والمعلومات الشخصية للأفراد من إساءة إستخدام بنوك المعلومات .

ثانياً :- تجريم حالات جمع البيانات الشخصية دون سبب مشروع مثل التداول غير المرخص به للمعلومات والإفشاء غير المشروع للمعلومات ، وإستخدام المعلومات في غير الغرض المخصص لها .

ثالثاً :- إخضاع أجهزة بنوك المعلومات لنظام قانوني دقيق من الترخيص للمحافظة على سرية البيانات والمعلومات المخزنه فيها، وفرض عقوبات مشددة في حالة إفشاء هذه المعلومات .

## بسم الله الرحمن الرحيم

### موضوع الدراسة :—

اهتمت المجتمعات منذ القدم بموضوع الحياة الخاصة ، وعملت جاهدة على حمايتها بوسائل شتى ، فالحق في الخصوصية قديم قدم البشرية ، وهو يقوم على حماية ذلك الجانب من حياة الإنسان والذي لا يرغب في اطلاق الغير عليه أو لا يرغب في أن يكون موضوعاً للحديث من جانب الناس ، فهو حق الإنسان في الخلوة أو في الذود عن فرديته ، وبمعنى آخر حقه في أن يعيش كما يريد في ذاته دون أن ترصده الأعين أو تلوكة الألسن أو تتلصص عليه الأذن .

وإذا كانت الحياة الخاصة موضوعاً للإهتمام منذ القدم ، فإن هذا الاهتمام قد تزايد في المجتمعات الحديثة ، حيث شغل موضوع الحق في الخصوصية ديزاً هاماً على الصعيد القانوني فانشغل به الفقه والقضاء في الدول الحديثة بغية توفير الحياة اللازمة له ، وتدخلت يد المشرع لتكرس له هذه الحماية ، سواءً على الصعيد المحلي أو على الصعيد الدولي .

ولعل هذا الاهتمام يرجع إلى ما للحق في الخصوصية من ارتباط وثيق بمسألة أخرى بعيدة الأثر في حياة الفرد في المجتمع الذي يعيش فيه إلا وهي حرية وما يترتب عليها من صون لكرامته واحترام لأدميته ، فلا يتطفل عليه المتطفل فيما يرغب في الاحتفاظ به لنفسه ، ولا تنتهك خصوصياته ، فليس هناك حق أعلى وأسمى من الحق في الخصوصية لما له من ارتباط وثيق في حرية الفرد (1).

(1) د. ممدوح خليل بحر ، حماية الحياة الخاصة في القانون الجنائي ، دراسة مقارنة ، رسالة دكتوراة ، كلية الحقوق ، جامعة القاهرة ، ١٩٨٣ ، ص ٩-١٠ .



فالحق في الخصوصية جوهر الحرية ، ويمكن أن يكون مرادفاً لمفهوم الحرية على أساس أن الحرية تعني مكنة مطالبة الآخرين بالامتناع عن التدخل ويفترض الحق في الخصوصية هذه المكنة أيضاً ولهذا يتفق مع الحرية إلى حد بعيد فيمكن أن تكون الخصوصية حقاً على مستوى القانون الخاص وعلى مستوى القانون العام أيضاً ، أي أن الإخلال بالحق في الخصوصية قد يقع من جانب الأفراد أو من الدولة<sup>(١)</sup> ، بيد أن هذا لا يعني التطابق التام بين الحرية والحق في الخصوصية . ويمكن القول أن الحق في الخصوصية يهدف إلى كفالة أسرار الفرد وخصوصياته ولا يثار هذا الحق إلا بصدد جوانب من الحرية تتسم بممارستها بمنأى عن الآخرين ، أما الحرية فتهدف إلى كفالة جوانب أخرى غير الحق في السرية والخصوصية ، كحرية العمل وحرية التجارة وما إلى ذلك ، ويفترض الحق في الخصوصية قدراً أكبر من عزلة الفرد وانسلاخه عن الآخرين ، في حين أن الحرية تمكن الفرد من مواجهة الآخرين والاحتكاك بهم مع التزام الكافة بالامتناع عن التعرض للفرد في ممارسته لهذه الحريات<sup>(٢)</sup> .

وللحق في الخصوصية أهمية بالنسبة للفرد وبالنسبة للمجتمع في ذات الوقت ، لأنه يكفل للفرد عدم تدخل الآخرين في حياته الخاصة مما يؤدي إلى أن يظل الفرد قادراً على العطاء متمتعاً بصفائه النفسي ، ويشعر من خلال احترام أسرار وجوده الذاتي مصوناً ، كما أنه يستطيع مراجعة نفسه ومحاسبتها إذا اختلى إليها ، فيصبح ضميره يقظاً ومن ثم يستطيع الشخص أن يسهم في تطور مجتمعه وتزداد لديه القدرة على الابتكار والإبداع ، وهذا كله يعود بالنفع على الفرد والجماعة<sup>(٣)</sup> .

وليس من شك أيضاً حيث شكل الفرد على مر الأحقاب محور الاهتمامات التشريعية لمختلف مصادرها الدولية والوطنية ، لتشريعات تسعى في تنظيماتها إلى حمايته وتحقيق مصالحه ، التي هي في النهاية تمثل مجموعة من مصالح المجتمع ككل بحيث يكون من السهل الميسور دائماً إقامة نوع من التوازن العادل بين هاتين المصلحتين في كل مرة يقع بينهما تعارض ، وتحقيقاً لذلك شهدت كل العصور محاولات

(١) د. نعيم عطية "حق الأفراد في حياتهم الخاصة" مقال منشور في مجلة إدارة قضايا الحكومة ، العدد الرابع ، السنة الحادية والعشرون ، سنة ١٩٧٧ ، ص ٨٠ .

(٢) المرجع نفسه ، ص ٨١ .

(٣) د. احمد فتحي سرور ، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد ، العدد الرابع والخمسون ، ص ٣٥ وما بعده .

من جانب التشريعات تهدف الى حماية الفرد من الاعتداءات التي تقع على حقه في حياته الخاصة .

تطور مفهوم الحق في الخصوصية وعلاقته ببنوك المعلومات .

كان للأحقاب التاريخية المتلاحقة أثرها المباشر في بلورة الفكرة الأساسية حول مدلول الخصوصية ، ففي غضون المرحلة القديمة عرف الحق في الخصوصية بمعنى الخصوصية المادية ، والتي مفادها حق الفرد بالشعور في انه تجنب تطفل المتطفلين أو تعكير الفضوليين لصفوة خلوته ووحدته التي بذل لها أسباباً مادية تعزله عن عالمه الآخر ، الأمر الذي أدى إلى اتساع معنى الخصوصية وفقاً لهذا المدلول لتصبح للأشخاص لا للمكان ، وما يترتب عليه من بطلان الربط بين الخصوصية وحق الملكية للمكان<sup>(١)</sup> .

تطور مدلول الخصوصية في المرحلة الحديثة ، حيث أضيفت إليها مفاهيم جديدة تركز على شمولها لعناصر عديدة خلافاً لما كان عليه الحال في المرحلة القديمة ، وكان للتطور التكنولوجي أثره المباشر على حقوق الأفراد وحياتهم الأساسية - بما فيهم حقهم في حماية حياتهم الخاصة - الأمر الذي حدا بالبعض إلى القول أن الحق في الخصوصية يشمل خمسة عناصر تدرج جميعها تحت إطار المفهوم الشمولي له<sup>(٢)</sup> ، وهي : " ١- الحماية من سوء استخدام اسم أو صورة المرء لأغراض تجارية. ٢- الحماية من عملية النشر على الملأ بشكل محرج ، ٣- الحماية من نسبة رأي أو موقف لشخص معين وهو لا يؤمن به أصلاً ، ٤- الحماية من التدخل في شؤون الفرد الخاصة ، ٥- الحماية من كشف أو القدرة على منع الاتصالات الخاصة بين الزوجين أو الطبيب أو مريضه أو المحامي وموكله " <sup>(٣)</sup> .

(١) د. محمد عبد المحسن المقاطع ، حماية الحياة الخاصة للأفراد وضمائنها في مواجهة الحاسوب الالي ، مطبوعات جامعة الكويت ، الطبعة الاولى ، ١٩٩٢ ، ص ٥٢ .

(٢) د. سامر دلالة ، مشكلات الحق في الخصوصية في ظل الاستخدامات اللامنهجية لبنوك المعلومات ، دراسة مقارنة ، بحث مقدم للنشر في مجلة اليرموك ، جامعة اليرموك ، ٢٠٠٧ ، ص ٥ .

(٣) د. المقاطع ، مرجع سابق ، ص ٣١-٣٢ .

ويعتبر الحاسوب ثورة التكنولوجيا الحديثة والذي سهل الكثير من الأمور وتجاوز عقبات كنا نراها في الماضي من ضروب المستحيل ، ومن أخطر آليات التكنولوجيا المعاصرة تهديداً لحياة الإنسان في أخص شؤونها وأكثرها التصاقاً به (٤) .

كيف لا وهو الجهاز الذي بواسطته أصبح ممكناً للحكومة ، والأفراد ، والمؤسسات داخلياً وخارجياً ، أن تعرف وتجمع وتحلل وتوزع وتتبادل عن الفرد ، كل ما يخص شؤون حياته الماضية والحاضرة فضلاً عن أنماط سلوكه المستقبلية ، بما يجعل الإنسان مجرداً من جميع السواتر أمام هولاء جميعاً ، وهو يعتقد أن كل ما عرف عنه لا يتجاوز أمور بسيطة في أحيان محددة ، إن لم يكن يعتقد أنها لا تزال من أخص خصوصياته التي لم ولن يعلم بها أحد من الناس (٥) .

إن بنوك المعلومات اليوم فيما تحتوي عليه من معلومات عن الفرد وما يخزن عنه من بيانات تشكل عنصر تضيق وتقليل من انطلاقات الفرد وإبداعه ومشاركته في شؤون الحياة العامة ، والسبب الأساسي في ذلك يرجع إلى انه أصبح محورياً لعمليات آلية مختلفة تمسه في كل جانب من جوانب حياته المتشعبة ، فالحاسوب يقوم بجمع وتخزين ومعالجة ونشر المعلومات الشخصية للأفراد ، وكل أمر من هذه الأمور يشكل خطراً بشكل أو بآخر على حياة الإنسان الخاصة ويهددها . لذا فإن الفرد يصبح أسيراً للمعلومات التي جمعتها هذه الآلة عنه ، ورصدت كل تحرك من تحركات حياته أو تعرف مما يقوم به .

ومن الجدير بالذكر أن هذه الدراسة للمعلومات الشخصية للأفراد ترتبط بموضوع علمي وأساليب تكنولوجية حديثة ، فهي ليست دراسة تقليدية لمفهوم خصوصية الأفراد ، وإنما لوسائل تكنولوجية جديدة ومتطورة يمكن من خلالها انتهاك وتهديد خصوصيات الأفراد وتبادل المعلومات الشخصية وتداولها بطرق غير مصرح للآخرين الوصول إليها .

فإذا كان لبنوك المعلومات جانبها الإيجابي ، فهي من ناحية أخرى لها جانب سلبي يتمثل في تهديدها لأسرار خصوصية الفرد ، لما لها من قدرة فائقة على جمع

(٤) Donsia Renee Strong “The Computer Matching and Privacy Protection Act of 1988 : Necessary Relief From the Erosion of privacy Act of 1974 P .397

نقلًا عن المقاطع /المرجع نفسه ، ص ٣٧ .

(٥) المرجع نفسه ، ص ٣٧- ٣٨ .

أكبر قدر من المعلومات واسترجاعها في أقصر وقت ممكن ، مما يمكن بمساعدتها من ترجمة حياة الفرد في أقل من ثانية، والتي كانت يكسوها في الماضي ثوب ثقيل ، وظلال كثيفة لا تسمح لأي فرد بالكشف عنها، إلا أنها أصبحت أمام هذه البنوك شفافة واضحة وضوح الشمس دون أي غطاء يحجبها أو يحميها<sup>(١)</sup> .

### أهمية الدراسة :

مما سبق يتضح لنا أن الحق في الخصوصية من الحقوق الأساسية التي لا غنى عنها في حياة الفرد ومن بعده المجتمع الذي يعيش فيه .

فالحق في الخصوصية ضرورة إنسانية ذات طابع اجتماعي ، كما انه مظهر حقيقي لحرية الإنسان ، التي هي قوام حياته ووجوده ، و أساس بنيان المجتمع الديمقراطي السليم ، وهي الحقوق السابقة على وجود الدولة ، لا تخلقها الدوائر بل تنظمها ، ولا توجد القوانين بل توفق بين شتى مناحيها تحقيقاً للخير المشترك للجماعة ورعاية للمصالح العام<sup>(١)</sup> .

من اجل ذلك كله تحرص المجتمعات السوية على كفالة الحق في الخصوصية ، وتعتبره حقاً مستقلاً ، ولا تكتفي بسن القوانين لحمايته بل تسعى إلى ترسيخه في الأذهان لغرس القيم الأخلاقية التي تصدر عن الفرد نزعة ذميمة إلى التطفل و خدش أسرار الغير<sup>(٢)</sup> .

غير ان معطيات العصر قد تغيرت وتعددت أمور الحياة الاجتماعية ، وتعرضت معها خصوصيات المرء لمظاهر وأشكال مختلفة من الاعتداء دون أن تتقف القوانين الطبيعية حائلاً دون ذلك ، واصبح هناك ما يمكن أن يسمى بأزمة الحياة الخاصة .

(١) د. أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، دراسة مقارنة ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٨٩ ، ص ٦  
(٢) عدلي حسين " الحماية الجنائية الإجرائية لحرمة الحياة الخاصة " بحث مقدم إلى مؤتمر الحق في حرمة الحياة الخاصة المنعقد بكلية الحقوق ، جامعة الإسكندرية في الفترة من ٤-٦ يونيو ، ١٩٨٧ ص ٢١ .  
(٣) د. ادم عبد البديع ادم ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠ ، ص ٤ .

ولعل أهمية هذه الدراسة تبرز من خلال (٣) :-

أولاً :- الوقوف على الآثار المترتبة على اتساع دائرة التطور التكنولوجي وما ترتب عليه من نتائج تمثلت في اعتماد الكثير من الشركات والمؤسسات الخاصة والحكومية على الحاسبات التي لها قدرات كبيرة ومتميزة في جمع وتخزين واسترجاع ونقل كم هائل من البيانات الخاصة بأفراد المجتمع .

ثانياً :- الآلية التي يتم عن طريقها جمع هذه البيانات والتي قد تكون غير مشروعة في بعض الأحيان ، وهو ما يجعل فرص الوصول إليها على نحو غير مأذون به ويفتح مجال أوسع لإساءة استخدامها أو توجيهها توجيهاً منحرفاً أو خاطئاً أو مراقبة الأفراد وتعريه خصوصياتهم أو الحكم عليهم حكماً خفياً من واقع سجلات البيانات الشخصية المخزنة .

وتغدو أهمية الموضوع من كون المعلومة قوة ، وتمثل قيمة اقتصادية مستحدثة ، مما ينبغي معه إحقاق مبدأ الحق في المعلومات ، وذلك بتحقيق التوازن بين الاستخدام الحر والكامل للمعلومات ، وبين الحقوق والحريات والمصلحة العامة ، بحماية من تتعلق بهم المعلومات من المساس بشرفهم أو اعتبارهم أو حرمة حياتهم الخاصة ، أو استخدام هذه المعلومات على نحو غير مشروع من شأنها أن تهدد مصالح الأفراد المختلفة(٤) .

(٣) الدلالة ، مرجع سابق ، ص ٢ .  
(٤) د. احمد عوض بلال ، محاضرات في النظرية العامة للجريمة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة، ٢٠٠١، ص ٥٤ .

## مشكلة الدراسة :

لا يستطيع أحد أن ينكر الإيجابيات الكثيرة لبنوك المعلومات ، لكن هذه الثورة في المعلومات والمعرفة قد تنعكس سلباً على حرية الأفراد أو التطفل على حياتهم الخاصة ، والتسلل إلى أدق التفاصيل عن حياتهم والتي يجب أن تكون بعيدة كل البعد عن أعين الآخرين في حالة استخدام هذه البنوك .

إن مشكلة الدراسة الرئيسية تتوقف على كيفية التعرف على مدى الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات .

وتتفرع من هذه المشكلة إشكالية ثانوية تتمثل في التساؤل التالي :

كيف يمكن لبنوك المعلومات أن تشكل خطراً أو تهديداً للمعلومات الشخصية للأفراد ؟

وللإجابة عن التساؤل يمكن لنا أن نجمل الأخطار التي تسببها بنوك المعلومات للفرد عندما تنتهك معلوماته الشخصية بالنقاط التالية :

١. أن الكثير من المؤسسات الكبرى والشركات الحكومية والهيئات الخاصة ، تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل ، .... الخ ، وتستخدم الحاسبات وبنوك المعلومات في تخزينها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به ، ويفتح مجالاً أوسع لإساءة استخدامها.

٢. إن المعلومة الشخصية التي كانت فيما قبل منعزلة متفرقة ( مشتتة ) ، والتوصل إليها صعب متعذر ، تصبح في بنوك المعلومات المركزية مجمعة متوافرة متكاملة سهلة المنال ، متاح أكثر من ذي قبل استخدامها في أغراض الرقابة على الأفراد.

٣. هناك نظام المشاركة الزمنية (الإنترنت) والذي يسمح عن طريق شبكة اتصالات واسعة بالتعامل مع البيانات مباشرة والحصول على المعلومات

المطلوبة في اقصر وقت ممكن ، هذه الخطورة تكمن في أن من لديه مفتاح البيانات للكمبيوتر أي (الكود) يستطيع تجميع كل المعلومات التي تكون غالباً شخصية وخاصة عن شخص معين بشكل لم يكن متاحاً على الإطلاق من قبل.

### عناصر المشكلة :

تنهض عناصر المشكلة على مجموعة من التساؤلات التي مفادها البحث في المخاطر التي خلفتها بنوك المعلومات على الحماية الجزائية لاحق في الخصوصية ، ومن هذه التساؤلات :

- هل المبادئ القانونية المستقرة الآن قادرة على مواجهة التصدي لأخطار بنوك المعلومات ؟
- هل شكل استخدام هذه البنوك آلية للولوج إلى الأسرار والمعلومات المرتبطة بالحياة الخاصة بالأفراد ، أم أن الحماية التشريعية ساهمت في مواكبة كافة المستجدات في هذا الميدان ليتأتى من خلالها الاستثمار الأمثل لبنوك المعلومات في ظل تنامي التطور التكنولوجي ؟
- هل النصوص التقليدية في قانون العقوبات وقانون أصول المحاكمات الجزائية او في القوانين الخاصة كافية لحماية المعلومات وسرية البيانات في مواجهة أخطار بنوك المعلومات في حالة إساءة استخدام البيانات الشخصية ؟ أم انه يجب سن تشريعات جديدة لحماية خصوصية الفرد في مواجهة هذه الأخطار ؟

### أهداف الدراسة :

في ضوء المشكلات التي يثيرها موضوع "الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات" يمكننا أن نحصر أهداف دراستنا في ثلاثة أهداف رئيسية :-

١. مراعاة التوازن بين مصلحة الفرد في صون أسرار حياته الخاصة والحفاظ قدر الإمكان على معلوماته الشخصية من أخطار بنوك

المعلومات ، وبين مصلحة المجتمع في المساس بهذه الأسرار وكشفها في بعض الحالات الموجبة لذلك .

٢. بيان مواطن الضعف والقصور في تشريعات الدول التي التزمت الصمت نحو أخطار بنوك المعلومات على حق الفرد في خصوصية معلوماته ، حيث اكتفت هذه التشريعات بحماية الأسرار ، ومنها تشريعنا الأردني.
٣. تمكين الفرد من السيطرة على معلوماته الشخصية التي تسجل لدى بنوك المعلومات وذلك من خلال الضمانات المتاحة للأفراد .

وتحقيقاً للهدف المقصود من هذه الدراسة التي اتخذت الشخص الطبيعي محوراً لها ، فانه سوف ينصب اهتمامنا في هذا البحث إلى دراسة حماية المعلومات الشخصية للفرد وضماداتها في مواجهة بنوك المعلومات ، وما شكلته من تهديدات بالغة الخطورة عميقة الجراح على كيانه وكرامته .

#### التعريف بالمصطلحات :

وإذا كان موضوع الدراسة هو حماية المعلومات الشخصية في مواجهة بنوك المعلومات، فانه لا بد من توضيح ماهية المعلومة التي يتم تداولها عن الأفراد ، وتوضيح مفهوم بنوك المعلومات ، والمعالجة الآلية لهذه المعلومات ، ثم طبيعة العلاقة ما بين المعلومات الخاصة بالأفراد وبنوك المعلومات . وذلك على النحو الآتي :

أولاً : طبيعة المعلومات المتعلقة بالحياة الخاصة للأفراد .

يثور التساؤل في هذا الصدد حول ماهية المعلومات التي تعرض خصوصية الأفراد في إطار مجتمع المعلومات الإلكترونية لانتهاك ؟ فهل كل معلومة يتم تداولها في بنوك المعلومات تثير مسألة الخصوصية الشخصية؟! وكذلك هل يعتبر الرضا بإعطاء بيانات شخصية لهذه البنوك أو الجهات القائمة عليها رضاء بتداول هذه المعلومات؟!

نتفق مع من يرى أن المعلومات المجهولة - التي لا تدل على من تتعلق به - لا تثير أية صعوبة ، حيث أن المجهول لا خصوصية له ، ولكن الأمر يصدق في حالة المساس بالمعلومات المتعلقة بأفراد معينين ، مما يؤدي إلى المساس بخصوصياتهم ،



فتكون بذلك المعلومة اسمية ، إذا أنها تسمح بالتعرف على الشخص محل هذه المعلومة بطريقة مباشرة أو غير مباشرة<sup>(١)</sup> .

وقد تكون المعلومة موضوعية - لا تعكس آراء شخصية - أي تتعلق ببيانات مجردة مثل (الاسم ، الموطن ، الحالة المدنية ، الحالة الجنائية ) ، ومن ثم تعتبر من مميزات الشخصية لمن تتعلق به المعلومة .

وكذلك قد تكون المعلومة ذاتية - تحمل رأياً ذاتياً عن الغير - فمؤلفها يختلف عن الشخص موضوع المعلومة ، كالمقال الصحفي أو الملف الإداري<sup>(١)</sup> .

وإذا كانت المعلومة الموضوعية أو الذاتية غالباً ما تتعلق بالحياة العامة للأفراد ، فإن البيانات الاسمية المخزنة في بنوك المعلومات هي التي تمس الحياة الخاصة للأفراد ، والحق في الخصوصية المعلوماتية ، وهي مدار بحثنا .  
وتعرف البيانات الاسمية على أنها (( البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء ، كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية ، عندما تكون هذه البيانات محلاً للمعالجة الآلية ))<sup>(٢)</sup> .

ثانياً : موضوع حماية المعلومات الشخصية .

أن موضوع البيانات الاسمية المتعلقة بالحياة الخاصة ليست المعلومات المخزنة بحد ذاتها، إنما تتمثل في المصالح التي تتهددها هذه المعلومات غير الصحيحة أو المشوهة .

وكون الحق في المعلومات يصلح لان يكون محلاً للحقوق الشخصية والمالية ، فإنه يجب ان تحمي خصوصية الأفراد بقوانين حديثة ، وذلك بالتخلي عن حرفية النص الجنائي فيما يتعلق بالحماية الجنائية للحق في الخصوصية وعن العناصر المبهمه المكونة للجريمة<sup>(٣)</sup> ، للحفاظ قدر الإمكان على خصوصية المعلومات الخاصة بالأفراد من مخاطر بنوك المعلومات واستخداماتها المختلفة ، والتي غدت تقدماً للوسائل القامعة

(١) د. سعيد عبد اللطيف حسن ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت ( الجرائم الواقعة في مجال تكنولوجيا المعلومات ) ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ١٩٩٩ ، ص ٢٣ وما بعدها

(٢) د. حسام الدين كامل الاهواني ، "الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني" ، مجلة العلوم القانونية والاقتصادية ، العددان الأول والثاني ، ١٩٩٠ ، ص ٥ .

(٣) د. نائل عبد الرحمن صالح ، واقع جرائم الحاسوب في التشريع الجزائي الأردني ، ورقة عمل مقدمة إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، ٢٠٠٠ ، ص ١٠ .

(٣) د. سعيد عبد اللطيف حسن ، المرجع السابق ، ص ٣٣ .

للحرية الفردية إذا ما أسيء استخدامها . وهذا المساس بالمعلومات الشخصية للأفراد ، قد يكون مصدره هواة متطفلون لا يلحقون أي أذى بصاحب البيانات ولا يتسببون عادة بأية أضرار ، إنما يكون هدفهم إثبات مقدرتهم على التفوق التقني بحل رموز الشيفرة واختراق بنوك المعلومات ، أو للتسلية باستخدام هذه المعلومات بإزعاج الآخرين ، وقد يكون مصدر هذا المساس أيضاً أشخاص مخربون يجدون من بيئة التقنية المكان الملائم لممارسة هواياتهم الإجرامية بخفاء ، وذلك بالاعتداء على البيانات الشخصية للآخرين وانتهاكها بشتى الصور<sup>(٤)</sup> .

### ثالثاً : مفهوم بنوك المعلومات .

أما المراد ببنوك المعلومات فهو تكوين قاعدة بيانات تفيد موضوعاً معيناً وتهدف لخدمة غرض معين ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة ، ومن ثم يمكننا القول بان هناك بنكاً للمعلومات المالية أو القانونية أو الطبية أو السياسية أو الأمنية أو العسكرية ، كما انه من الممكن أن يشتمل بنك المعلومات على أكثر من نوع من أنواع البيانات السابقة ، مثل بنوك المعلومات القومية التي تتضمن قواعد بيانات عن نواحي الحياة المختلفة السياسية والأمنية والصحية والاقتصادية ، ... الخ<sup>(١)</sup> .

" تغدو المعلومات بهذا المفهوم مستقلة في مدلولها عن البيانات التي تشكل في الأصل مدخلات للنظام المعلوماتي ليتم معالجتها باستخدام الحاسوب والخروج بمعلومات عن الموضوع أو الفرد أو القطاع الذي تعلق به تلك البيانات" <sup>(٢)</sup> .

### رابعاً : المعالجة الآلية لنظم المعلومات :

ويقصد بها مجموعة العمليات التي تتم آلياً ، أي باستخدام الحاسوب الآلي وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات الاسمية ، وكذلك مجموعة العمليات التي تتم آلياً بغرض استغلال المعلومات وخصوصاً عمليات الربط والتقريب وانتقال المعلومات الاسمية ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومة ذات دلالة خاصة.

(٤) [http : // www. FTC Gov/ Reports / Privacy htni.](http://www.FTC.Gov/Reports/Privacy.html)

نقلاً عن / محمد امين الشوابكة ، جرائم الحاسوب والانترنت ، الطبعة الاولى ، دار الثقافة ، عمان ، ٢٠٠٤ ، ص

(١) د. أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، مرجع سابق ، ص ٤٨ .

(٢) الدلالة ، الحق في الخصوصية في ظل الاستخدامات اللامنهجية ، مرجع سابق ، ص ٧ .

ومن الجدير بالذكر أن بنوك المعلومات تمثل مخرجات حصيلة المعالجة الآلية للبيانات المدخلة للحاسوب أو لأنظمة المعالجة الآلية للبيانات .

## منهج الدراسة :

يسهم كلاً من المنهج الوصفي والمنهج الوظيفي التحليلي في معالجة هذه الدراسة بصورة يتحقق في ضونها وضع الظاهرة في محيطها القانوني لرسم معالم السلوك غير المشروع وقدرة النصوص القانونية على استيعاب هذا النشاط بالتجريم والعقاب.

## خطة الدراسة :

لقد تم تقسيم خطة الدراسة إلى فصلين ، تناولت في الفصل الأول منها مخاطر بنوك المعلومات على حق الفرد في خصوصية معلوماته ، حيث أن المعلومات التي يمكن أن تسجل عن الأفراد لدى هذه البنوك كثيرة ومتنوعة ، حيث تشمل جميع نواحي الحياة الخاصة للأفراد ، مما يؤدي بالنهاية إلى انتهاك خصوصية الفرد إذا ما تم الإساءة إلى هذه المعلومات واستخدامها في غير الغرض الذي خصصت من أجله ، وتم تداولها بطرق غير مسموح للآخرين الوصول إليها .

ثم تم تقسيم هذا الفصل إلى مبحثين ، تناولنا في المبحث الأول منه الأشخاص الذين يمكنهم الاعتداء على حق الفرد في خصوصية معلوماته ، حيث أن هذا الاعتداء قد يقع من الهيئات العامة في الدولة أو من الهيئات الخاصة وهي مؤسسات المجتمع المدني الخاصة أو قد يقع من الأفراد أنفسهم . كما تم التطرق إلى بيان طرق الاعتداء على هذه المعلومات في المبحث الثاني.

إما فيما يتعلق بالفصل الثاني من هذه الدراسة وهي مبادئ حماية المعلومات الشخصية وضماناتها في مجال تجميعها في بنوك المعلومات ، فقد تم تقسيمه إلى مبحثين ، ثم التركيز في المبحث الأول على مبادئ الحماية لهذه المعلومات ثم خصص المبحث الثاني إلى الضمانات المعطاة للأفراد من أجل السيطرة على المعلومات الشخصية المسجلة عنهم لدى أجهزة بنوك المعلومات .

### تقسيم الخطة:

وتحقيقاً لما سبق والتزاماً به ، سيتم عرض الدراسة في فصلين متتاليين ، وذلك وفقاً لخطة منهجية تمكن من الإلمام بجزئيات الموضوع والربط بينها وتتابعها ، وذلك على النحو الآتي :-

## الفصل الأول

مخاطر بنوك المعلومات على حق الفرد في خصوصية معلوماته

"وفيه مبحثين "

المبحث الأول : الأشخاص الذين يرتكبون الاعتداء على حق الفرد في معلوماته الشخصية.

المبحث الثاني : طرق الاعتداء على المعلومات الشخصية .

## الفصل الثاني

مبادئ حماية المعلومات الشخصية و ضماناتها

في مجال تجميعها في بنوك المعلومات

"وفيه مبحثين "

المبحث الأول : مبادئ حماية المعلومات الشخصية في بنوك المعلومات .

المبحث الثاني : الضمانات المتاحة للفرد في السيطرة على معلوماته الشخصية .

والدراسة الماثلة هي اجتهاد من عمل البشر ، والعمل البشري عرضة للخطأ والصواب بطبيعته، فالكمال لله وحده عز وجل ، فأن اجتهادنا فأصبنا فلنا أجران ، وأن اجتهادنا فأخطأنا فلنا اجر واحد.

ونسأل الله العلي القدير أن يكون عملنا خالصاً لوجه الكريم ، وان نكون قد حققنا ما قصدنا إليه من نفع وخير لأجيال هذه الأمة ، انه نعم المولى ونعم النصير .

الباحث

## الفصل الأول

# مخاطر بنوك المعلومات على حق الفرد في خصوصية معلوماته

### تمهيد وتقسيم :

كتب الفقيه الفرنسي ميلر ( Mellor ) في عام ١٩٧٢ ( ان الكمبيوتر بشرايته التي لا تشبع لجمع المعلومات على نحو لا يمكن وضع حد لها، وما يتصف به من دقة وعدم نسيان ما يخزن فيه، قد تنقلب حياتنا رأسا على عقب يخضع فيها الأفراد لنظام رقابة صارم ويتحول المجتمع إلى عالم شفاف تصبح فيه بيوتنا ومعاملاتنا المالية وحياتنا العقلية والجسمانية عارية لأي مشاهد )<sup>(١)</sup> .

ولو كان يدرك ( ميلر ) ما ستؤول إليه فتوحات عصر المعلومات ، وما سيتحقق في بيئة شبكات المعلومات العالمية ، والعالم الإلكتروني لأدرك أن ما قاله أصبح يسيراً على التقنية ، فهي فيما وصلت إليه الآن من مراحل التطور أمكنها أن تجمع شتات المعلومات عن كل فرد وتحيلها إلى بيان تفصيلي بتحركاته وهواياته واهتماماته ومركزه المالي، ... الخ .

فتقنية المعلومات الجديدة يمكنها خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي تم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ، ومن قبل الشركات الخاصة ، ويعود الفضل في هذا إلى مقدرة الحوسبة الرخيصة ، وأكثر من هذا فإنه يمكن مقارنة المعلومات المخزونة في ملف (مؤتمت) بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة نسبياً ، ان هذا بوضوح يكشف إلى أي مدى يمكن أن يكون تهديد الخصوصية .

(١) Arther Mallor "The assault of Privacy Computers. Data Banks and ssiers Aun Arbor the University of Michigan Press . 1970. P4 نقلًا عن / ممدوح بحر ، حماية الحياة الخاصة في القانون الجنائي ، مرجع سابق ، ص ١٦ .

وبفعل الكفاءة العالية لوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات ، اتجهت جميع دول العالم بمختلف هيئاتها ومؤسساتها إلى إنشاء قواعد البيانات لتنظيم عملها ، واتسع على نحو كبير استخدام الحواسيب لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية ، ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في هذا المضمار ، ظهر بشكل متسارع أيضاً، الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية ، هذا الشعور نما وتطور بفعل الدلالات الواقعية للاستخدام غير المشروع للبيانات الشخصية واتساع دائرة الاعتداء على حق الأفراد في الحياة الخاصة، مما حرك الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأن مراعاتها حماية الحق في الخصوصية ، وبالضرورة إيجاد نوع من التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية ، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها .

ويمكننا فيما يلي إجمال المعالم الرئيسية لمخاطر الحواسيب وبنوك المعلومات على الحق في الخصوصية بما يلي .:

أولاً : قدرة الحاسبات الإلكترونية على جمع البيانات المتعددة ، وتحليلها وتنظيمها وتوزيعها وتخزينها في بطاقات أو على شرائط بالنسبة للمشروعات أو الأفراد أو الدولة، والتي بمساعدتها يمكن ترجمة حياة الفرد في اقل من ثانية ، وذلك باسترجاع هذه المعلومات مما يشكل خطراً حقيقياً على حياة الأفراد الخاصة<sup>(١)</sup> . كما أن إنشاء الدولة لبنوك المعلومات القومية لا يقتصر على جمع البيانات وعلاجها واستقلالها ، ولكنه يقدم هذه المعلومات للسلطات عندما تحتاجها ، فيمكن للدولة أن تنشئ ملفات تتضمن المعلومات الشخصية عن بعض الأفراد اللازمة للتحقيق أو تحديد هويتهم ، بالإضافة إلى أن استخدام الأجهزة الإلكترونية التي تعمل عن بعد يتيح جمع أكبر قدر من المعلومات الخاصة عن الأفراد من بنوك متعددة ومتفرقة دون علم الشخص ، مما يعد اعتداءً على حياته الخاصة<sup>(٢)</sup> .

(١) قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، مرجع سابق ، ص ٥٧ .  
(٢) د. آدم عبد البديع آدم ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠ ، ص ٤٩٩ .



ثانياً: إن المخاطر المحدقة في الحق في الخصوصية تكمن حدثها في أن بنوك المعلومات قد ساهمت في جمع اكبر قدر ممكن من المعلومات عن الأفراد مع عدم معرفة اوجه استخدامها في المستقبل ، ولا يقتصر هذا الخطر على البنوك العامة ، ولكن يمتد إلى البنوك الخاصة كالبنوك التي تنشئها شركات التأمين وشركات الأموال ، إذ تقوم بجمع بيانات تتعلق بعملائها ، سواء في حياتهم الشخصية أو الصحية ودرج معاملاتهم ومنافسيتهم وعماليتهم، مما يهدد سرية حياتهم الخاصة ، وكذلك استخدام البيانات التي تم جمعها عن الأفراد في غير الغرض المخصص لها ، الأمر الذي يحتم ضرورة وضع التشريعات الخاصة لحماية البيانات الشخصية وضمان عدم إساءة جمعها ، أو استخدامها في غير الغرض المعدة من اجله (١) .

ثالثاً:- ومن الأخطار الناشئة أيضاً عن استخدام بنوك المعلومات - بالنسبة للبيانات الداخلة أو المعلومات الخارجة - ما يعرف بالأخطاء التقنية والبشرية المقصودة وغير المقصودة والتي تقع عند تغذية الحاسوب بالمعلومات أو عند إعادة تنظيمها أو تقويمها ، أو الأخطاء الناتجة عن الأعطال الميكانيكية والكهربائية ، كما انه من السهل تغيير البيانات عند التغذية دون اكتشافها(٢) .

وإذا كان موضوع هذا الفصل ينصب على بيان خطورة بنوك المعلومات على حق الفرد في خصوصية معلوماته ، فانه من الضروري إظهار الأشخاص الذين يمكنهم الاعتداء على حق الفرد في خصوصية معلوماته عن طريق الاعتداء الذي يقع من قبل الهيئات العامة والخاصة وكذلك بالنسبة للاعتداء الذي يقع من الأفراد أنفسهم، وكذلك تبين طرق الاعتداء على المعلومات الشخصية، ويظهر ذلك من خلال استخدام المعلومات لغير الغرض الذي جمعت من اجله ، ومن خلال التداول غير المرخص به للمعلومات وكذلك بالنسبة للأخطاء في المعلومات والبيانات، والإفشاء غير المشروع للبيانات .

(١) Alan F. Westin "Privacy and Freedom".op.cit,p68 Est، jean Rivero،op.cit,p.66

نقلًا عن / د. آدم عبد البديع ، مرجع سابق ، ص ٥٩ .

(٢) المرجع نفسه ، ص ٥٠٠ - ٥٠١ .

وفي ضوء ما تقدم سنقسم دراستنا في هذا الفصل الى المبحثين التاليين :-

المبحث الأول :- الأشخاص الذين يمكنهم الاعتداء على حق الفرد في معلوماته الشخصية.

المبحث الثاني :- طرق الاعتداء على المعلومات الشخصية.

## المبحث الأول

الأشخاص الذين يمكنهم الاعتداء على حق

الفرد في خصوصية معلوماته الشخصية

### تمهيد وتقسيم:—

ان التطور العلمي والتقني له اكبر الاثر في حياة الفرد والمجتمع ، حيث انه بفضل هذا التطور الهائل في المعرفة والمعلوماتية ، اصبح التوصل الى البيانات عن الاشخاص اكثر يسراً وسهولة من ذي قبل بفضل استخدام الحاسوب في النظام الموحد لبنوك المعلومات ، فتم استخدامه في كافة اوجه الحياة المختلفة فهناك بذلك للمعلومات الطبية او السياسية او المالية ، ... الخ

الا ان الامر يزداد خطورة عندما يتم استخدام البيانات بطرق غير مشروعة من شأنها ان تهدد مصالح الافراد الخاصة .

ومما لا شك فيه فإن الدولة باعتبارها صاحبة الولاية على الافراد تستطيع بكافة مؤسساتها وهيئاتها الحكومية ان تجمع عن الفرد بيانات متعددة ورسم صورة واضحة المعالم عن كافة الانشطة التي يمارسها ، سواء المتمثلة بالانشطة السياسية أو الاجتماعية أو الاقتصادية، ... الخ .

الا ان انشاء الدولة لبنوك المعلومات لا يقتصر على جمع البيانات وعلاجها واستقلالها، ولكنه يقدم هذه المعلومات للسلطات عندما تحتاجها ، فيمكن للدولة ان تنشئ ملفات تتضمن معلومات شخصية عن بعض الافراد اللازمة للتحقيق او تحديد هويتهم بالاضافة الى ان استخدام الاجهزة الالكترونية التي تعمل عن بعد يتيح جمع اكبر قدر من المعلومات الخاصة عن الافراد من بنوك متعددة ومتفرقة دون علم الشخص ، مما يعد اعتداءً على حياته الخاصة .

اما على صعيد الهيئات والمؤسسات الخاصة فإن المخاطر التي تحدثها لا تقل اهمية عن تلك التي تسببها الممارسات والتشريعات الحكومية ، فالشركات التجارية اصبحت تعرف عن الافراد ادق التفاصيل في حياتهم اليومية نتيجة لجمعها بيانات



ويكون الفرد عارياً أمام هذه البنوك ، التي أصبحت تعرف عنه كل شيء ، حيث تقوم بتجميع هذه المعلومات ونقلها وتوزيعها وتحليلها وتبادلها<sup>(٢)</sup>.

والأمثلة عن المعلومات الشخصية التي تقدم للسلطات العامة كثيرة منها شهادات الميلاد والزواج والوفاة والحالة الصحية والشهادات العلمية، والخدمة العسكرية، وطلبات استخراج جوازات السفر وطلبات الاضرائب وطلبات جميع أنواع الرخص... الخ.

وتعتمد هذه السجلات على معلومات اختيارية مقدمة من الفرد او من اقاربه ، وهذا على خلاف ما يكون من سجلات سرية جمعتها سلطات البوليس أو المخابرات أو الجهات الأمنية الأخرى .

ومن الأمثلة الصارخة في إساءة استخدام البيانات والمعلومات الشخصية المتعلقة بالأفراد، ما حدث في الولايات المتحدة الأمريكية في عام ١٩٧٠ ، عندما قام جهاز الخدمة السرية بجمع وتسجيل البيانات عن الأشخاص المشتبه فيهم ، ثم تقسيمهم وفقاً لهذه البيانات إلى ثلاث طوائف :- الأولى الخاصة بالمشتبه فيهم لارتكاب الاغتيالات السياسية ، أما الطائفة الثانية فيمثلها الأشخاص الذين يهاجمون سياسة الدولة من خلال آرائهم ، وأخيراً الطائفة الثالثة وهم الأشخاص الذين يهددون امن الدولة بواسطة إحداث الاضطرابات أو الدعوة إليها بين العاملين<sup>(١)</sup>.

"ولقد عمدت بعض الدول إلى استحداث برنامج على مستوى النظام الحكومي، يقوم بعمليات رقابة على سلوكيات الأفراد من خلال ما يتجمع عنهم من معلومات بواسطة أنظمة البطاقة الموحدة ، ففي الولايات المتحدة الامريكية مثلاً تم استخدام الرقم الموحد للضمان الاجتماعي للقيام بعمليات التحكم والمراقبة على الأفراد في شؤونهم الحياتية استناداً إلى مبررات عديدة مثل الحفاظ على الأمن القومي ، أو لمصلحة دولة الرفاه الاجتماعي"<sup>(٢)</sup> .

ولقد سارت المانيا على النهج ذاته إذ ان المعلومات المجمعة والخاصة بشؤون الضمان الاجتماعي ، يتم استخدامها لأغراض السيطرة والتحكم في حياة الأفراد

(١) د. ادم عبد البديع ادم ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، مرجع سابق، ص ٤٩٦ .

(٢) المرجع نفسه ، ص ٥٠١ .

(٣) المقاطع ، حماية الحياة الخاصة للأفراد وضماداتها في مواجهة الحاسوب الالي ، مرجع سابق ص ٤٨ .

ومراقبة أنماط سلوكهم ، وهذا الأمر يتكرر أيضا بالنسبة لهذه المعلومات التي تستخدم في مجال الضرائب أيضا<sup>(٣)</sup> .

أما في استراليا فان الحكومة الفيدرالية منذ عام ١٩٨٥ اقترحت استحداث ما يسمى ببطاقة استراليا ، والذي تأمل الحكومة هناك أن يكون نظاماً فريداً في تعريف الشخص ، والذي يسهم بشكل فاعل في تسهيل الوصول لجميع المعلومات التي يحتاج إليها مكتب الضرائب ، خصوصاً وانه سيسمح بسهولة في الاتصال مع عدد كبير من الملفات التي تشتمل على معلومات مختلفة عن دافعي الضرائب<sup>(٤)</sup> .

ولكن إزاء تلك المخاطر والانتهاكات ، هل يحق للدولة ممثلة بحكوماتها ان تكون بمنأى عن البيانات الشخصية لمواطنيها ؟ وهل تشكل أفعال التخزين للبيانات التي تقوم بها الحكومات انتهاكاً صريحاً لخصوصيات الأفراد، ولا سيما مع بدء العمل بما يعرف بالحكومات الالكترونية؟! .

نتفق مع من يرى أن "الإرادة هي الأداة الأساسية في تحديد ما يدخل في إطار الخصوصية ومقدار ونوعية المعلومات المباح المساس بها عن طريق تخزين ومعالجة تلك البيانات إلا أن المصلحة العامة تبقى فوق كل اعتبار، لذا يجوز تخزين البيانات متى استلزمت ذلك من تهديد لحياة الأفراد الخاصة وحياتهم"<sup>(١)</sup> .

ويرى البعض<sup>(٢)</sup> "أن التخوف من المساس بالحياة الخاصة والحريات الشخصية ، يكون أشده في مواجهة الدولة وأجهزتها ،حيث أن سهولة انتقال وتبادل المعلومات بين الحاسبات الآلية وبنوك المعلومات التابعة للسلطة التنفيذية وأجهزتها، قد يؤدي إلى التأثير على رسم السياسة العامة للدولة فيما لو احتكرت تلك المعلومات ، الأمر الذي يؤدي إلى أن تصبح القوه الفعلية في النظام السياسي لدى من يسيطر على هذه المعلومات من خلال الخبراء والفنيين التابعين للسلطة التنفيذية ، من خلال إشرافهم على الحاسبات الآلية وبنوك المعلومات ، مما يؤدي بالنتيجة الى الإخلال بالتوازن المطلوب بين السلطات لصالح السلطة التنفيذية" .

(٣) المرجع نفسه ، ص ٤٨ .

(٤) المرجع نفسه ، ص ٤٨ .

(١) الشوابكة ، جرائم الحاسوب والانترنت ، مرجع سابق ، ص ٦٧ .

(٢) المرجع نفسه ، ص ٦٧ .

وبناءً على ما تقدم فإن التشريعات في مختلف دول العالم يجب عليها ان تتصدى لمثل هذا الأمر، بحيث تنظر إلى المؤسسات الحكومية المختلفة ، على أنها أجهزة منفصلة ومستقلة عن بعضها البعض بالنسبة للمعلومات التي قامت بتجميعها ، بحيث يقيد استخدامها للغاية او الهدف الذي جمعت من اجله ، وذلك صونا لحق الأفراد في حماية معلوماتهم الشخصية<sup>(٣)</sup> .

والخلاصة في رأينا ان الاعتداء قد يتحقق من مختلف الهيئات والمؤسسات الحكومية عندما تقوم بجمع بيانات عن الأفراد ، خاصة إذا لم تستخدم هذه البيانات في إطارها الصحيح. فالدولة باعتبارها صاحبة الولاية العامة على الأفراد فانه من المصلحة العامة فيها ان تقوم بجمع بيانات ومعلومات عن أفرادها مما يساعد في عملية البناء والتخطيط والنهوض بالمواطنين الى مستوى عال من الرقي والازدهار ، فعندما تقوم السلطة العامة بالتعداد العام للسكان مثلا فانها تجمع عن الأفراد سجلا كاملا من البيانات التفصيلية والتي تتعلق بالحالة المدنية والصحية والتعليمية والسياسية ، وتقوم بتفريغ هذه البيانات في بنوك خاصة ، تسمى بنوك المعلومات المركزية ، والتي من خلالها تستطيع معرفة تحركات كل فرد من أفراد المجتمع ، الأمر الذي يشكل إعتداءً وافتئاتاً على خصوصية الفرد في حالة إساءة استخدام هذه المعلومات في غير الغرض الذي جمعت من اجله . وعلى الدولة ان تقيم نوعا من التوازن بين حقها في الاطلاع على هذه المعلومات من اجل النفع العام ، وبين حق الفرد في المحافظة على هذه المعلومات التي أخذت عنه ، وحقه في الاطلاع عليها وتصويبها .

وتأسيسا على ما تقدم فانه لا يجوز للدولة احتكار المعلومات ، كما انه يجب التأكيد على شفافية الإدارة ، حيث أن المعلومة التي تؤخذ عن الفرد تمثل قيمة وثروة تستطيع أن تصل إلى حد أن تصبح سلطة ، فعن طريق جمعها وترتيبها وحفظها ومعالجتها ثم استخدامها ، ونشرها أو على العكس الاحتفاظ بها ، يمكن المساس من خلالها بحقوق وحرية الأفراد . وفي المقابل يوجد للأفراد حق حماية المعلومات الشخصية والمحافظة على خصوصياتهم وأسرارهم في مواجهة التطفل الاناجم عن وسائل التقدم التكنولوجي في الرقابة وجمع المعلومات ومعالجتها وخصوصا بنوك المعلومات.

(٣) المقاطع ، مرجع سابق ، ص ١٥٧ .

ومن ثم اتخذت الدول المتقدمة مثل الولايات المتحدة الأمريكية وكندا ، والسويد وإنجلترا وألمانيا وفرنسا الاحتياطات ووسائل الحماية اللازمة لمواجهة التطور التكنولوجي لعصر المعلومات ، كما بذلت الجهود لإعداد التشريعات الملائمة لمواجهة هذا التطور ، وحماية المعلومات الخاصة للمواطنين ، وفي ذات الوقت فتح المجال لحصولهم على المعلومات واستخدامها الاستخدام الأمثل في التخطيط ورسم السياسة والاقتصاد<sup>(١)</sup> . وهذا ما سنعالجه في الفصل الثاني من هذه الدراسة .

---

(١) عمرو احمد حسبو ، حماية الحريات في مواجهة نظم المعلومات ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ ، ص ٩٣ .



## المطلب الثاني

### الاعتداء الذي يقع من الهيئات الخاصة

لقد شهد العالم اليوم ثورة هائلة في تكنولوجيا المعلومات سواء المتمثلة بالإنترنت أو الحاسوب أو بنوك المعلومات المركزية، هذا التدفق الهائل في المعلومة عن الأفراد يجعل من الشركات التجارية الكبرى والمؤسسات الخاصة التي تعنى بشؤون الفرد أن تجمع عنه معلومات شخصية وتقوم بتخزينها في بنوك معلومات خاصة لديها ، ثم تعمل على تحليل هذه المعلومة ونقلها وتبادلها وتوزيعها ونشرها ، مما يؤثر على حياة الفرد وتجعله في موضع حرج أمام الآخرين .

ان القدرة الخيالية التي وصل إليها الحاسوب في تجميع معلومات مختلفة عن الفرد في كل تحرك من تحركات حياته أو تصرف مما يقوم به، تجعل الفرد أسيرا للمعلومات التي جمعتها هذه الآلة . فلقد غدا من السهل بفضل الذكروت البنكية المذهلة وأشرطة الفيديو تسجيل أنشطة الفرد وإعادة بنائها وعرضها بتفاصيل وبيطء وبدقة متناهية<sup>(1)</sup>.

فالمخاطر التي يمكن أن تحدث على صعيد المؤسسات الخاصة، لا تقل عن تلك التي تسببها الممارسات والتشريعات الحكومية ، فالشركات التجارية أصبحت تعرف عن الأفراد أدق التفاصيل في حياتهم اليومية، نتيجة لجمعها معلومات خاصة ومعينة . وخير مثال على ذلك ما حدث في فرنسا يوضح خطورة المؤسسات والشركات التجارية حيال جمعها المعلومات عن الأشخاص ، وتتلخص وقائع هذه الحادثة ، أن شخصا فصل من وظيفته سنة ١٩٦٥ ، ومكث بعدها خمس سنوات وهو يبحث عن عمل ، ولكن طلباته التي قـدرت بـ

(٦٢٥) طلبا في مختلف الشركات والمؤسسات رفضت جميعا . وأخيرا اكتشف سنة ١٩٧١ أن الشركات والمؤسسات التي تقدم إليها، عندها بطاقات سبق أن أعدت بواسطة شركتين تجاريتين ينحصر نشاطهما في جمع المعلومات ، وقد كانت البطاقة

(1) المقاطع ، مرجع سابق ، ص٤٨

الخاصة به تحوي معلومات سيئة بشأنه ، وتحوي هذه البطاقة على شخصية الموظف وأعماله السابقة التي كان يمارسها ومدى تقدمه في العمل من عدمه ، وأجره وإجازاته وأسباب الإقالة وأحيانا آراؤه السياسية أو معتقداته الدينية وانتماءاته النقابية (١).

ومن الأمثلة الصارخة أيضا على عدم الاهتمام بخصوصية المعلومات في عالم الكمبيوتر وبنوك المعلومات ما حدث في الولايات المتحدة الأمريكية لأحدث هيئات نظام البيانات، عندما أنهت أعمالها فعرضت للبيع بأعلى سعر محتويات معلوماتها عن ثلاثة ملايين مواطن (٢).

ان الأخطار التي يسببها التقدم في مجال بنوك المعلومات تؤدي إلى فقدان الخصوصية في الشؤون المختلفة من حياة الأفراد ، وفقدان خصوصية المعلومات من أكثر المخاطر التي يسببها عصر المعلومات ، وتزداد خطورة جمع هذه المعلومات الشخصية بسبب ظهور مثل هذه الشركات الخاصة والتي تعمل في مجال الأمن ، حيث تقوم بتجميع بيانات عن الأفراد لوضعها تحت تصرف من يريد ان يعرفها نظير دفع مقابل مالي ، فقد أصبح وجود مثل هذه المعلومات الشخصية مهددا للحياة الخاصة بالنسبة للفرد العادي وكذلك بالنسبة للشخصيات العامة، هذا التهديد لحياة الأفراد يتحقق سواء كانت هذه المعلومات خاطئة أو كانت صحيحة ، ما دام صاحب الشأن يعترض على من يقوم بجمعها وتخزينها أو يقوم بتزويد الآخرين بها بدون مسوغ قانوني مقبول (٣).

وفي رأينا فان استخدام بنوك المعلومات في شتى ميادين الحياة دون وضع الضمانات القانونية اللازمة لحماية الأفراد ، يمثل تهديداً وخطرا داهما على حق الفرد في خصوصية معلوماته، هذا الخطر يتمثل في السماح بجمع البيانات او المعلومات عن الأشخاص مع عدم معرفة أوجه استخدامها في المستقبل ، ولا يقتصر هذا الخطر على البنوك العامة ، ولكن يمتد الى البنوك الخاصة كالبنوك التي تنشئها شركات التأمين وشركات الأموال والبنوك والمشروعات الهامة ، إذ تقوم بجمع بيانات تتعلق بعملائها،

(١) Yves Madiot : (Droit de l homme et liberte s publiques) Masson droit et sciences .  
economiques paris 1976-p-233

نقلاً عن / د.مدوح خليل بحر ، مرجع سابق ، ص ١٦-١٧ .

(٢) المرجع نفسه ، ص ١٧

(٣) د.غنام محمد غنام ، الحماية الإدارية والجنائية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر ، مجلة الأمن والقانون ، العدد الثاني ، أكاديمية شرطة دبي ، السنة الحادية عشر ، يوليو ٢٠٠٣ ، ص ٨٧ .

سواء في حياتهم الشخصية او الصحية وحجم معاملاتهم ومنافسيهم وعمالدهم، مما يهدد سرية حياتهم الخاصة، وكذلك استخدام البيانات التي تم جمعها عن الأفراد في غير الغرض المخصص لها، او استخدامها في غير ما يلائم صاحبها او يوافق صاحب الشأن او دون رضائه، بالإضافة الى جمع بيانات او معلومات عن شخص دون سبب مشروع، مما يعد اكبر انتهاكا للحياة الخاصة، وتهديدا للحريات الفردية، الأمر الذي يحتم ضرورة وضع التشريعات الخاصة لحماية البيانات الشخصية وضمان عدم إساءة جمعها أو استخدامها في غير الغرض المعدة من اجله.

### المطلب الثالث

#### الاعتداء الذي يقع من الأفراد

في ظل التطور العلمي الحديث في مجال بنوك المعلومات المنتشرة لدى الأجهزة العامة والخاصة في الدولة الواحدة ، ونتيجة لامتلاك الأفراد أجهزة الحاسب الآلي في البيوت ، وتطور خدمة الانترنت فانه أصبح من السهولة على هؤلاء الأفراد امتلاك المعلومة ، حيث يتم تخزينها وجمعها وتصنيفها ثم تحليلها واحياناً قد يتم نشر هذه المعلومة للكافة مما يلحق الضرر المادي والمعنوي لهؤلاء الأشخاص الذين تم اخذ المعلومة عنهم .

خلاصة ذلك الأمر ان هناك اعتداء وافتنات قد يقع من الأفراد أنفسهم عند امتلاك المعلومة وتوظيفها في غير الغرض الذي خصصت من اجله أو في حالة إساءة استخدام مثل هذه المعلومات الشخصية ، والتي جمعت بطريقة مشروعة أو غير مشروعة .

وقد يقع الاعتداء من نوعين من الأفراد .

أولاً:- الاعتداء الذي يقع من الأفراد القائمين على بنوك المعلومات :-

حين تقوم الدولة بإنشاء بنوك للمعلومات ، فانه لا بد من ان يكون هناك أشخاص قائمين على هذا العمل ومشرفين على هذه البنوك من حيث تخزين المعلومة ومعالجتها واحياناً تحليلها ، فمثل هؤلاء الأشخاص عليهم واجب الاحتفاظ بسر المهنة وعدم

إفشاء الأسرار أو إعطاء معلومات عن شخص ما من شأنه ان تلحق به الأذى والضرر وتعرضه إلى بغض الناس واحتقارهم . فمثلاً عند إنشاء البنوك الطبية ، فإنه هناك سجلاً كاملاً عن الشخص ، يحتوي على معلومات تفصيلية عن سيرته المرضية ومراحل تلقيه العلاج وسفراته إلى الخارج ، مثل هذه البيانات لو عرفت عن الشخص فإنها تجعله في موضع ازدراء أمام الآخرين ، خاصة ان الكثيرين من الأفراد لا يحبذون ان تعرف عنهم مثل هذه الأمور لأنها تعتبر من صميم المعلومات الشخصية والخاصة والتي يجب ان تكون بعيدة كل البعد عن أعين المتطفلين .

ولحماية المعلومات الشخصية من تسريبها للغير عن طريق القائمين على بنوك المعلومات ، فإن معظم الدول قد نظمت قوانين خاصة تحظر على مثل هؤلاء القيام بإفشاء الأسرار ومنها (قوانين سر المهنة ، قانون الإحصاءات العامة ، قانون الاتصالات ، قانون حماية المؤلف ،.... الخ) .

ثانياً :- الاعتداء الذي يقع من قبل الهواة المتطفلين :-

لقد اصبح التوصل إلى البيانات والمعلومات عن الأفراد اكثر سهولة من ذي قبل ، بفضل استعمال الحاسب الإلكتروني في النظام الموحد لبنك المعلومات ، كما ازدادت الحاجة إلى السرية كي يتسنى حماية الأفراد والحفاظ على خصوصية معلوماتهم ، فالمعلومات التي كان من الصعب التوصل إليها نظراً لصعوبة الكشف عنها ، أصبحت سهلة المنال ، بتطبيق النظام الموحد للبنوك الذي ساعد على توافر وتكامل الحقائق عن الأفراد ، ومن بين النتائج المخيفة لسوء استعمال هذا النظام ، إمكان التعرف على الأفراد من خلال اخذ المعلومات الخاصة بأشخاصهم<sup>(1)</sup> .

ويستطيع الفرد المتطفل التوصل إلى المعلومة عن طريق الدخول إلى مواقع بعض الأشخاص على الانترنت وتجميع اكبر قدر ممكن من المعلومات بطريقة ذكية ، خاصة وان كثير من الأشخاص قد يدلون بمعلومات شخصية عنهم ، لجهات معينة وهم على ثقة بان هذه المعلومات لا تستخدم إلا بطريقة مشروعة ، لكن الأمر يزداد خطورة إذا تسلل هؤلاء الهواة والمتطفلين إلى مواقع تلك الجهات بطريقة يمكنهم من خلالها حل رموز تلك الشيفرة ، واخذ ما يريدونه من معلومات سجلت عن الأفراد ، مما يتسبب بالحاق الأذى والضرر فيما لو تم تسريب هذه المعلومات للغير .

(1) د. مبدر سليمان الويس اثر التطور التكنولوجي على الحريات الشخصية في النظم السياسية ، رسالة دكتوراة ، كلية الحقوق ، جامعة القاهرة ، سنة ١٩٨٢ ، ص ١٢٦

وقد ظهرت أحداث شهيرة في حقل الاعتداء على البيانات الخاصة للأفراد ، من بينها على سبيل المثال - الحادثة التي حصلت في جنوب أفريقيا حيث أمكن للمعتدين الوصول إلى الأشرطة التي خزنت عليها المعلومات الشخصية بمصابي أمراض الإيدز وفحوصاتهم ، وقد تم تسريب هذه المعلومات الخاصة والسرية إلى جهات عديدة<sup>(2)</sup> .

ومن الحوادث الشهيرة أيضاً حادثة حصلت عام ١٩٨٩ عندما تمكن أحد كبار موظفي أحد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية ، بان تسرب إليها شريطاً يحتوي على أرصدة عدد من الزبائن<sup>(1)</sup> .

وخلاصة الأمر في رأينا ان أي معلومة يمكن جمعها من قبل الفرد قد تؤثر على سمعة الأفراد التي جمعت عنهم مثل هذه المعلومات وبالتالي يكون الشخص مكشوفاً أمام الآخرين، فمثلاً المعلومات التي تجمع آلياً عن الفرد خصوصاً في حالة كون الشخص مريضاً ( بمرض الإيدز ) فانه سيكون في حالة مكشوفة تماماً أمام شركات التأمين ، وهو أمر سيجعل الأطباء يترددون كثيراً في تقديم رعاية وخدمات طبية أفضل لحساسية المعلومات التي يريدون اطلاع الغير عليها ومن ثم تقليل فرص العلاج الأفضل للشخص المريض .

كما ان تسريب معلومات عن زبائن بعض البنوك قد يضر بمصالحهم الشخصية ، نتيجة لمعرفة سلطة الضرائب عن وضعهم المالي ، مما يؤدي إلى فرض ضرائب بمبالغ كبيرة جداً وهذا يؤثر على القدرة المالية لهؤلاء الأشخاص . كما انه قد يؤدي إلى اهتزاز الثقة فيما لو تم معرفة الوضع المالي لهم وخصوصاً إذا كان الشخص تاجراً مما يؤثر على سمعته في الأوساط التجارية وعزوف الكثير عن التعامل معه ، نتيجة اختلال الثقة التجارية مما يلحق الأذى والضرر به .

وتأسيساً لما سبق فانه لا بد من وضع الضمانات الكافية لحماية البيانات والمعلومات والمعطيات الشخصية من افتتات الغير سواء أكانوا أفراداً أم شركات خاصة، وهذا ما سوف نعالجه في الفصل الثاني من هذه الدراسة .

(2) [http:// www. Privacy international .org](http://www.Privacyinternational.org)

(1) نفس المرجع السابق .

## المبحث الثاني

### طرق الاعتداء على المعلومات الشخصية

#### تمهيد وتقسيم :

الأصل أن تستخدم البيانات أو المعلومات التي تؤخذ عن الفرد في إطارها الصحيح وفي الغرض الذي جمعت من أجله ، ولذلك فإنه لا يجوز جمع المعلومات وتداولها بطرق غير مشروعة من شأنها أن تؤثر على سمعة الأفراد وتضر بمصالحهم المختلفة السياسية منها والاجتماعية والمالية.

إلا أن الفرد قد يتعرض في حياته لمخاطر الاعتداء والانتهاك لمعلوماته الشخصية نتيجة لسلوك بعض الشركات الخاصة والمؤسسات الكبرى لطرق غير مشروعة في التعامل مع هذه البيانات، فبنوك المعلومات الموجودة لدى الأجهزة الحكومية ولدى الشركات الخاصة ، سهلت فرص الوصول إلى المعلومة والتقاطها من قبل المعتدين ، بعد أن كانت معلومة مشتتة ومبعثرة في ملفات يدوية مختلفة .

وفي مجال التطور العلمي والتكنولوجي فإن هذه البنوك يمكنها تخزين أكبر قدر ممكن من المعلومات عن ملايين الأشخاص ، والاحتفاظ بها إلى الأبد ، واستخراج بيانات كافية - وفي أي وقت - عن أي إنسان من المسجلين بها وتعريته حياته بكشف تفاصيل سابقة على وقت استخراجها بزمان طويل مما قد يسبب له أضرار بليغة يتعذر أو يستحيل إصلاحها فضلاً عن أن المعلومات الشخصية التي كانت فيما قبل منعزلة متفرقة والتوصل إليها صعباً أو متعزراً ، تصبح في هذه البنوك مجمعة متوافرة متكاملة سهلة المنال في أي وقت ، متاح أكثر من ذي قبل استخدامها في أغراض الرقابة على الأفراد .

وفي مجال معالجة البيانات ، تتبدى المخاطر المهددة للمعلومات الشخصية للأفراد عند ربط الحاسبات بعضها ببعض ، أو ربطها بحاسب مركزي أو بشبكات عامة للاتصال ، حيث يتسنى بذلك تبادل المعلومات فيما بين المراكز المعلوماتية المتباينة مكانياً والمختلفة من حيث أغراض تخزين البيانات بها ، وربط هذه المعلومات بعضها البعض واستكمالها وتحليلها ومعالجتها على نحو يتيح التوصل إلى معلومات جديدة من شخص أو مجموعة أشخاص .

وبالرغم من ان المعلومات الشخصية للأفراد محاطة بسياسات محكمة من السرية وعدم إفشاء بعض المعلومات إلا في الحالات المحددة والتي يجيزها القانون لمصلحة القطاع الحكومي إلا انه يمكن اختراق هذا الحاجز من السرية والتسلل إلى أدق المعلومات وأكثرها خطورة على حريات الأفراد من قبل المعتدين سواء أكان قطاعاً عاماً أم قطاعاً خاصاً أو أفراد عاديين وبطرق مختلفة.

وسوف ندرس تباعاً طرق الاعتداء على المعلومات الشخصية للأفراد في أربعة مطالب، مخصصاً لكل طريق من هذه الطرق مطلباً مستقلاً لدراسته ، وعلى النحو التالي :-

**المطلب الأول :- استخدام المعلومات المجمعّة عن الفرد لغير الغرض الذي جمعت من أجله .**

**المطلب الثاني :- التداول غير المرخص به للمعلومات .**

**المطلب الثالث :- الإفشاء غير المشروع للمعلومات .**

**المطلب الرابع :- الأخطاء في المعلومات والبيانات .**

## المطلب الأول

استخدام المعلومات المجمعة عن الفرد لغير الغرض الذي جمعت من أجله

ان جمع بيانات عن الافراد وتخزينها لدى بنوك المعلومات دون معرفة الهدف او الغرض من جمعها قد يرتب مخاطر واثار من شأنها ان تؤثر على سمعة هؤلاء الاشخاص وتضر بمصالحهم المختلفة ، الامر الذي يستدعي من الجهات القائمة على بنوك المعلومات ، ان تستخدم هذه البيانات في اطارها الصحيح وان لا تتجاوز الهدف الذي جمعت من اجله .

ومن الجدير بالذكر ان المؤسسات الحكومية والشركات الخاصة قد تجمع بيانات عن الافراد ، كاليانات المتعلقة بالاحصاءات العامة ، فمثل هذه البيانات المخزنة في بنوك المعلومات يجب ان تستخدم ضمن الهدف المحدد لها ، وان لا تتجاوزه ، اما اذا تجاوزت الهدف كأن تستخدم لفرض ضرائب معينة على الافراد ، او لاغراض تجارية من قبل الشركات او لترتيب عبيء مالي ، فانها بذلك تكون قد انحرفت عن الغرض الذي من اجله جمعت هذه البيانات (١).

بمعنى انه لا يجوز استخدام البيانات الشخصية المجمعة الكترونياً في غير الاغراض الذي جمعت من اجلها ، ما لم يتم الحصول على اذن مسبق من اصحابها ، ويجب وضع الضمانات القانونية ضد افشائها او نقلها الى من لا يحق لهم معرفتها .

وتجدر الإشارة هنا ان " مكتب التحقيقات الفدرالية (FBI) في أمريكا يحتفظ بملفات للتعرف على الشخصية ، وتكمن خطورة هذه الملفات على الفرد في حالة قيام الإدارة بتزويد بعض الأجهزة الفدرالية أو المحلية بتلك المعلومات ، وقد تصل هذه المعلومات إلى شركات وهيئات خاصة ، وجميع مثل تلك الاستخدامات غير المتوقعة تؤدي إلى إيذاء الفرد وتقليل فرص تمتعه بحقوقه على وجهها الأكمل ، بل وتصبح قييدا

(١) John H. f . Shattuck "Right of Privacy" 1966 .p.155-156  
نقلاً عن / المقاطع ، مرجع سابق ، ص ٩٧



على حرّيته فيما يريد القيام به من أمور . فالأمر الذي لا جدل فيه ان نوع و حجم المعلومات التي يعطيها الفرد عن نفسه تختلف من جهة لأخرى وذلك وفقاً للهدف الذي دفع الفرد إلى إعطاء تلك المعلومات" (٢) .

فعلى سبيل المثال ينص قانون الإحصاءات العامة المؤقت رقم ٨ لسنة ٢٠٠٣ في مادته الحادية عشر(١) على عدم جواز استخدام المعلومات والبيانات التي جمعت عن الأفراد لأغراض الإحصائية في أي غرض آخر ، كان يستخدم للإدانة الجنائية ، أو فرض الرسوم أو ضرائب معينة ، وهو مسلك لا يساورنا شك في سلامته وصوابه في حماية حقوق الأفراد وحرّياتهم وحماية خصوصية معلوماتهم(٢) .

ان نوع وضخامة المعلومات التي يعطيها الفرد عن نفسه تختلف من جهة لأخرى وذلك لتحقيق الغرض الذي وضعت من اجله ، خاصة وانه إذا أدركنا ، بان شبكة تداول المعلومات تتيح إيصال المعلومات إلى جهات أو أشخاص قد يوقعون أضراراً بالفرد ويلحقون تجاوزات على حرّيته.

فإذا جمعت معلومات لغرض محدد من قبل شخص ما ولهدف محدد ، ثم وصلت هذه المعلومات إلى شخص آخر يجمع معلومات لغاية أخرى ، فان تجميع هذه المعلومات إلى تلك تتيح للحائز فرص كبيرة وخطيرة لإيقاع الضرر بالفرد ، لان الحائز الأول قد يفقد السيطرة عليها وتقع رحمة الحائز الثاني .

وفي التشريع المقارن نجد أن المشرع الفرنسي قد نص على جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية في المادة (٢٢٦) - (٢١) من قانون العقوبات الفرنسي التي نصت على " يعاقب بالحبس مدة خمس سنوات وغرامة ثلاثماية الف يورو كل من حاز بيانات اسمية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو أي إجراء آخر من اوجه المعالجة ، إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقاً للقانون أو بالقرار الصادر من اللجنة الوظيفية للمعلومات والحرّيات الذي تجيز المعالجة الإلكترونية من اجل

(٢) المرجع نفسه ، ص ٩٧ .

(١) المادة ١١/أ من قانون الإحصاءات العامة الأردني لعام ٢٠٠٣ تنص على "تعتبر سرّية جمع المعلومات والبيانات الفردية التي تقدم للدائرة والمتعلقة بأي مسح أو تعداد ، ولا يجوز لها أو لأي من العاملين لديها ، تحت طائلة المسؤولية القانونية ، اطلاع أي شخص أو جهة عامة أو خاصة عليها ، أو الكشف عنها كلياً أو جزئياً أو استخدامها لأي غرض غير إعداد الجداول الإحصائية " .

(٢) المقاطع ، حماية الحياة الخاصة للأفراد وضمّاناتها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ٩٩ .

الأبحاث العلمية وفي المجالات الصحية ، أو في الأخطار المسبق على القيام بالمعالجة" (١).

ويتضح من النص ان لهذه الجريمة ركنين : أحدهما : مادي يتمثل في إساءة استغلال البيانات والآخر معنوي يتخذ صورة القصد الجنائي ، ونعرض بالدراسة لهذين الركنين ، كما نبين العقوبات المقررة لمرتكبي هذه الجريمة .

أولا : الركن المادي

يتحقق الركن المادي لهذه الجريمة بمجرد الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات (٢).

والغرض أو الغاية هي موضوع المعالجة الإلكترونية ، أي الغرض المتوخى من علاج البيانات الشخصية وهي المبرر الوحيد لمعالجة البيانات الاسمية الإلكترونية (٣) .

وتفترض جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الاسمية الحصول ابتداءً على هذه المعلومات أو البيانات بصورة مشروعة ، أي بإذن من اللجنة الوطنية للمعلومات والحريات ، ولكن الجاني ينحرف عن الغرض المقصود منها .

وعلى سبيل المثال لا الحصر نجد أن الجاني يعد مرتكباً للنشاط المادي لهذه الجريمة فيما لو استغل البيانات الخاصة في الكشف عن مصادر ثروته أو لمعرفة مركزه المالي أو في الاستدلال عليه لخدمة مصلحة الضرائب (٤) .

(١) وقد أحوالت إلى هذا النص المادة (٤٤) من قانون ٦ يناير ١٩٧٨ والتي تنص على ان : " يعاقب بالحبس من سنة إلى خمس سنوات والغرامة من عشرين ألف فرنك إلى مائتي ألف فرنك كل شخص حائز لبيانات اسمية بقصد تسجيلها أو تصنيفها أو نقلها أو معالجتها تحت أي شكل وانحرف عن الغاية أو الغرض المحدد ."

(٢) ممدوح محمد المسلمي ، مشكلات البيع الإلكتروني عن طريق الانترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، سنة ٢٠٠٠ ، ص ٢١٣ .

(٣) آدم عبد البديع ، الحق في حرمة الحياة الخاصة ، ومدى الحماية التي يكلفها له القانون الجنائي ، مرجع سابق ، ص ٥٧٩ .

(٤) أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة

وبنوك المعلومات ، المرجع السابق ، ص ٩٩ .

ويثور التساؤل حول المرجع المنوط به تحديد الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الاسمية .

نجد ان المشرع الفرنسي في المادة ( ٢٢٦ - ٢١ ) قد اناط بالاضافة الى القوانين والانظمة التي تجيز جمع البيانات باللجنة الوطنية للمعلومات والحريات تحديد ما إذا كان فعل الجاني يشكل انحرافاً عن الغرض أو الغاية من فعل المعالجة ، وذلك بالرجوع إلى الطلب المقدم إليها مسبقاً والمحدد فيه الغاية أو الغرض من المعالجة الإلكترونية للبيانات ، وذلك وفقاً لنص المادة ( ٢٠ ) من قانون ١٩٧٨ .

والهدف من تحديد الغاية من المعالجة الإلكترونية ، تحقيق الرقابة لتجنب إساءة استخدام البيانات دون الحد من الإمكانيات المتاحة لاستغلال هذه البيانات .

ثانياً :- الركن المعنوي .

يتخذ الركن المعنوي في جريمة الانحراف عن الغرض أو المعالجة الإلكترونية للبيانات الشخصية صورة القصد الجنائي العام ، والذي يقوم بتوافر العلم والإرادة .

فيتعين أن يعلم الجاني بان من شأن فعله أن يشكل انحرافاً عن الغرض من المعالجة الإلكترونية للبيانات ، وان تتجه إرادته نحو ذلك (١).

ولا عبرة بالبواعث التي تدفع الجاني لارتكاب هذه الجريمة أو الغاية التي يهدف إليها سواء تمثلت بجر مغنم للجاني أو دفع ضرر عنه ، أو تحقيق مصلحة للغير .

---

(١) د. محمود نجيب حسني ، شرح قانون العقوبات ،

القسم العام ، الطبعة الخامسة ، دار النهضة العربية ،

القاهرة، سنة ١٩٨٥ ، ص ٦٠٨ .

### ثالثاً : العقوبة :

يعاقب المشرع الفرنسي كل من يرتكب جريمة الانحراف عن الغرض او الغاية من المعالجة الإلكترونية للبيانات الاسمية بالحبس خمس سنوات وبغرامة مليوني فرنك فرنسي ، وقد تشدد المشرع في عقوبة الحبس والغرامة لما تمثله هذه الجريمة من اعتداء جسيم على خصوصية البيانات والمعلومات الشخصية للأفراد .

أما في التشريع الجزائي الأردني ( قانون العقوبات ) فلم نجد نص عام حول مفهوم جريمة الانحراف عن الغاية أو الغرض من المعالجة الإلكترونية للبيانات الاسمية ، على غرار ما هو موجود في قانون العقوبات الفرنسي الجديد ، والذي يجرم مثل هذا الانحراف ويضع العقوبة المناسبة له ، بل وشدد المشرع من هذه العقوبة لما تمثله من اعتداء جسيم على خصوصية المعلومات بالنسبة للأفراد .

كما انه ليس ثمة قانون واحد عام لحماية البيانات الشخصية من مخاطر بنوك المعلومات والمعالجة الإلكترونية ، كما هو في الدول المتقدمة تكنولوجياً (٢) .

إلا انه يمكن الاستناد إلى نص المادة (١٥) فقرة (أ) من قانون الإحصاءات العامة الأردني المؤقت رقم (٨) لسنة ٢٠٠٣ ، والتي تنص على " أ . يعاقب بالحبس مدة لا تقل عن ستة اشهر ولا تزيد على سنة أو بغرامة لا تقل عن خمسمائة دينار ولا تزيد على ألف دينار أو بكلتا العقوبتين أي من موظفي الدائرة إذا ارتكب أيّاً من الأفعال التالية :-

١ . إفشاء أي معلومات او بيانات احصائية سرية بالمعنى المنصوص عليه في المادة (١١) (١) من هذا القانون أو سر من اسرار الصناعة او التجارة وغير ذلك من اساليب العمل التي تعتبر من أسراره ويكون قد اطلع عليها بحكم عمله.

(٢) مثل : أمريكا ، فرنسا ، النمسا ، استراليا ، السويد ، وغيرها .

(١) تنص المادة (١١) من قانون الإحصاءات العامة الأردني المؤقت رقم ٨ لسنة ٢٠٠٣ على " تعتبر سرية سرية جميع المعلومات والبيانات الافرادية التي تقدم للدائرة والمتعلقة بأي مسح او تعداد ولا يجوز لها او لأي

٢. تعمد الاحتفاظ بأي وثائق احصائية تحتوي على البيانات او تعمد اتلافها او تزويرها .

٣. اضاءة أي وثائق احصائية لها صفة سرية تحتوي على البيانات بسبب الاهمال".

ونتناول بالعرض للركن المادي وللركن المعنوي لهذه الجريمة ثم العقوبة المقررة لها.

أولاً : الركن المادي :-

يتحقق النشاط المادي لهذه الجريمة بمجرد الانحراف عن الغرض أو الغاية من جمع هذه البيانات ، حيث أن البيانات والمعلومات تجمع عن الأفراد ابتداءً من اجل إعداد الجداول الإحصائية فقط ، أما إذا انحرفت الدائرة عن هذا الهدف المحدد لها ، اما اذا انحرفت الدائرة عن الهدف المحدد لها وقامت باطلاع الغير الذي ليس له صلاحية الاطلاع على المعلومات المخزنة لديها فانها بهذا الفعل تكون قد شكلت اعتداءً على حقوق الافراد.

فالموظف الذي يعمل في الدائرة يعد مرتكباً للنشاط المادي لهذه الجريمة اذا اطلع أي شخص او جهة عامة او خاصة عليها أو استغل البيانات الخاصة للأفراد في الكشف عن مصادر ثروتهم او معرفة مراكزهم المالية ، او اطلع شركات التأمين عليها من اجل جر مغنم له .

---

لأي من العاملين لديها، تحت طائلة المسؤولية القانونية ، اطلع أي شخص او جهة عامة او خاصة عليها او الكشف عنها ، كلياً او جزئياً او استخدامها لأي غرض غير إعداد الجداول الإحصائية".

ثانياً :- الركن المعنوي :-

يتخذ الركن المعنوي في جريمة الانحراف عن الغرض أو الغاية في إعداد الجداول الإحصائية والتي يتم معالجتها إلكترونياً صورة القصد الجنائي العام<sup>(١)</sup> ، والذي يقوم بتوافر العلم والارادة .

فيتعين ان يعلم الجاني بان من شأن فعله نتيجة اطلاق أي جهة عامة او خاصة على هذه البيانات التي لها صفة السرية ان يشكل انحرافاً عن الغاية او الغرض من المعالجة الالكترونية للبيانات الشخصية ، وان تتجه إرادته نحو ذلك .

ثالثاً : العقوبة :-

يعاقب المشرع الأردني في المادة (١٥) من القانون المشار إليه ، كل موظف في دائرة الإحصاءات العامة قام بإفشاء أي معلومات او بيانات احصائية سرية بالمعنى المنصوص عليه في المادة (١١) او تعمد الاحتفاظ بأي وثائق احصائية تحتوي على البيانات ، او اضافة أي وثائق احصائية لها صفة سرية تحتوي على البيانات بسبب الاهمال ، بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن خمسمائة دينار ولا تزيد على ألف دينار أو بكلتا العقوبتين .

(١) د. كامل السعيد ، شرح الاحكام العامة في قانون العقوبات ، الطبعة الاولى ، دار الثقافة ، عمان ، ٢٠٠٢ ، ص ١٣٣ .

## المطلب الثاني

### التداول غير المرخص به للمعلومات

من المضار التي تلحق الفرد بسبب وجود معلومات مخزنة عنه آلياً في بنوك المعلومات هو "احتمالية حدوث تداول غير مرخص به لهذه المعلومات"<sup>(١)</sup> .

ويمكننا تصور هذا الضرر في أشكال عديدة منها :- "ان يحصل شخص ما وبأسلوب علمي وذكي على كلمة السر للملفات المخزنة آلياً في بنك من بنوك المعلومات المختلفة ، فهنا ينتهي الأمن للمعلومات ، بالرغم من ان الحاسب الآلي يحتاج لأشخاص ماهرين ليتمكنوا من الدخول على المعلومات المخزنة به ، والاطلاع عليها ، فالضرر الذي يتخوف منه هنا يتمثل بالتساؤل حول الضمانة من عدم حصول دخول غير مصرح به من الغير بواسطة جهاز أو أي أسلوب آخر"<sup>(٢)</sup> .

ان الدخول للبيانات والمعلومات المخزنة في بنوك المعلومات دون رخصة بذلك ، أو من قبل الأفراد غير المرخص لهم بذلك يعد انتهاكاً واعتداءً خطيراً على حق الفرد في خصوصية معلوماته الأمر الذي من شأنه ان يرتب أضراراً بالغة الخطورة على حقوق الأفراد من ذلك مثلاً النشر الواسع للمعلومة ، أو استغلالها تجارياً ، أو استخدامها في غير الغاية المحددة لها ، وبالواقع فان حصول مثل هذه الأحداث كثيرة ومتعددة ومن الملاحظ انه مهما حرصت الأجهزة على تأمين المعلومات بصورة سرية ومحكمة ، إلا ان هناك حالات خرق وانسياب لهذه المعلومات ، الأمر الذي يستوجب التيقظ إلى مثل هذه الأمور عما تلحقه من أضرار بالأفراد ، قد تنقل هذه المعلومات من أجهزة أخرى فتفقد استقلاليتها وتعرض أصحابها للأضرار .

لقد أفضى العلم الحديث إلى إمكانية قيام برامج استخدام مشترك لمعلومات مخزنة في كمبيوتر مركزي ، وهو ما يمكن صاحب هذا الكمبيوتر أو غيره ان يطلع على المعلومات من المشتركين معه ويتداولها ، ولذلك فان الشخص في حالة اشتراكه في

(١) Raymond Walks "The Protection of Privacy" , Sweet & Maxwell Limited , London , 1980 , P . 131-

132

نقلاً عن / المقاطع ، حماية الحياة الخاصة للأفراد وضمائنها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ٩٩ .

(٢) المرجع نفسه ، ص ١٠٠ .

هذه البرامج كان يتوقع الخصوصية لمعلوماته كأصل ، مما يجعل هذه المعلومات محمية قانوناً وفقاً لمبدأ الخصوصية الذي تنحصر حمايته عن الفرد عندما لا تكون الخصوصية متوقعة من قبله لما قام به من عمل أو أدلى به من بيانات<sup>(١)</sup> .

ولقد عمدت الكثير من التشريعات إلى حماية المعلومات من التعرض المسيء لأصحابها، فالتشريعات الأوروبية لحماية المعلومات مثلاً قدمت ضمانات لحماية هذه المعلومات، منها النصوص المتعلقة بتنظيم واستخدام المعلومات وتخزينها ، فضلاً عن إجراءات تامين المعلومات من الضياع أو التدمير أو الكشف ، لذلك يجب ان يتم تسجيل كل من حالات الكشف عن هذه المعلومات، وان يعلم الفرد عن حالات الاطلاع أو الدخول غير المسموح به على بياناته<sup>(٢)</sup> .

ومن الأمثلة الواقعية على ذلك ، ما قام به أحد التلاميذ في بريطانيا ، حيث تمكن من الدخول والوصول إلى معظم الملفات السرية المخزنة بكمبيوتر إحدى الشركات الكبرى والتي تدير نظاماً للمشاركين في خدمات الكمبيوتر ، وذلك بان حصل على كشوفات نظام التشغيل وتحليلها بالإضافة إلى الأرقام السرية الخاصة بالمشاركين ، والتي تتيح له الولوج إلى النظام والاطلاع على الملفات السرية الخاصة بهم<sup>(٣)</sup> .

وفي رأينا فان الدخول والتداول غير المرخص به للمعلومات من قبل الغير ، يؤدي إلى المساس بحقوق وحرية الأفراد ، خاصة حق الفرد في خصوصية معلوماته ، فعند تداول المعلومات التي أخذت عن شخص ما ، فان من شأنها ان تؤثر على سمعته وقد تلحق به الأذى والضرر الذي لا يمكن تعويضه في بعض الأحيان .

من هنا وجب على تشريعات الدول المختلفة ان تتصدى لمثل هذا الأمر ، وان تعالج في تشريعاتها حماية خصوصية المعلومات وتجرم العديد من صور السلوك التي من شأنها النيل أو المساس بحق الفرد في خصوصية معلوماته .

(١) المرجع نفسه ، ص ١٠٠

(٢) Michael Epperson "Transnational Contracts For Eguivalency of Data Protection . information services Secaring P . 161

نقلاً عن / المقاطع ، مرجع سابق ، ص ١٢٠ .

(٣) كمال احمد الكركي ، النواحي الفنية لإساءة استخدام الكمبيوتر ، بحث مقدم إلى ندوه " الجرائم الناجمة عن التطور التقني " المنعقدة بعمان في الفترة من (٢٨ - ٢٩) أكتوبر ١٩٩٨ ، ص ٥



وفي التشريع المقارن ، تعاقب اكثر هذه القوانين ، كما هو الحال في النمسا<sup>(١)</sup> وألمانيا<sup>(٢)</sup> وفرنسا، على الإفشاء أو الإفصاح أو الحصول أو الوصول غير المشروع إلى البيانات الشخصية التي تكون موضوعاً لمعالجة آدية . وتذهب بعض القوانين إلى تجريم شكل معين من أشكال الوصول أو الحصول على البيانات الاسمية بطريق الغش، كما هو الحال في قانون لوكسمبرج لسنة ١٩٧٩ الخاص بتنظيم استخدام البيانات الاسمية الذي يجرم الوصول إلى هذه البيانات باستخدام اسم مستعار أو صفة كاذبة<sup>(٣)</sup> .

وتشترك معظم قوانين حماية الخصوصية في تأثيم تسجيل ومعالجة البيانات الشخصية دون الحصول على ترخيص ، ويجرم أكثرها جمع أو تسجيل أو تخزين البيانات الشخصية بالذمة الحساسة أو وثيقة الارتباط بذاتية وكيان الإنسان كالبيانات المتعلقة بالأصول العرقية والمعتقدات الدينية والآراء السياسية ، وما أشبه ، كما يجرم كذلك الحصول على البيانات الشخصية بوسائل وطرق تدليسية غير مشروعة<sup>(٤)</sup> .

ونخلص من خلال دراستنا للتشريعات المقارنة ، ان المشرع الفرنسي قد وضع قانوناً خاصاً لحماية البيانات والمعطيات الشخصية من أخطار المعالجة الإلكترونية، وقد نص على جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص في المادة (٢٢٦ - ١٦) من قانون العقوبات الجديد وسنتناول هذه الجريمة بالتفصيل .

تنص المادة (٢٢٦ - ١٦) من قانون العقوبات الفرنسي الصادر سنة ١٩٩٤ على أن:- "يعاقب كل من يقوم ولو بإهمال بمعالجة إلكترونية أو يأمر بها للبيانات الاسمية دون مراعاة الإجراءات الأولية للقيام بها والمحددة في القانون بالحسب مدة ثلاث سنوات وبغرامة مقدارها خمسة واربعون الف يورو ."

(١) المادة (١/٤٨) من قانون حماية البيانات النمساوي الصادر في ١٨/أكتوبر ١٩٧٨ وتنص " على انه دون إخلال بأية عقوبة اشد ، يعاقب بالحسب مدة تزيد على سنة كل من أفشى عمداً أو استخدم بيانات معهود بها إليه ، أو مصرح له وحده، بسبب طبيعة عمله في مجال المعالجة الآلية للبيانات ، بالاطلاع عليها ، .....  
(٢) المادة (١/٤١) من قانون حماية البيانات الفيدرالي الألماني الصادر في ٢٧ يونيو ١٩٧٧ وتنص على ان يعاقب بالحسب مدة تزيد على سنة أو الغرامة " كل من قام بدون تصريح :  
١. بنقل أو إتلاف ٢. باسترجاع أو الحصول لنفسه ، من انظمة تخزين المعلومات القاصرة على مودعي هذه المعلومات ، على بيانات شخصية مشمولة بحماية هذا القانون وغير معروفة علناً "  
(٣) د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، بدون طبعة ، مكتبة الالات الحديثة ، اسبوط ، ١٩٩٢ ، ص ص ٣٨١ - ٣٨٣ .  
(٤) المرجع نفسه ، ص ٣٨٣ .

يتبين من خلال النص السابق انه يتعين لقيام هذه الجريمة توافر ركنين :-

الاول : مادي يتمثل في فعل المعالجة الإلكترونية للبيانات الاسمية دون مراعاة الإجراءات الأولية التي يتطلبها القانون ، والثاني :- معنوي يتخذ صورة القصد الجنائي وسوف نتعرض لهذين الركنين بالدراسة ، ثم نبين العقوبة المقررة لهذه الجريمة .

أولاً : صورة الركن المادي :

يتحقق النشاط المادي لهذه الجريمة بأية معالجة إلكترونية للبيانات الاسمية دون اتخاذ الإجراءات الأولية التي يتطلبها القانون ، فيلزمه لقيامه توافر عنصرين :-

١ . "سلوك إجرامي يتخذ شكل المعالجة الإلكترونية للبيانات الشخصية من حيث تسجيلها أو تحليلها أو تعديلها ثم حفظها أو محوها ، أو كل مجموعة من العمليات من ذات الطبيعة تحمل معالجة لهذه البيانات بقصد الربط بينها للحصول على معلومات شخصية . ويكون الفعل قد تم حتى لو كانت المعالجة باهمال من الفاعل" (١) .

٢ . "عدم مراعاة الشروط والإجراءات الأولية الواردة بالقانون رقم ١٧ لسنة ١٩٧٨ والخاص بالمعالجة الإلكترونية للبيانات الشخصية ، أي ان يتم إجراء المعالجة الإلكترونية للبيانات الشخصية دون إذن من " اللجنة الوطنية للبيانات والحريات " وفقاً لاحكام

(١٥ ، ١٦) من القانون المشار إليه" (٢) .

وتنص المادة (١٥) من القانون المشار إليه ( ٦ يناير ١٩٧٨ ) على انه بخلاف الحالات التي يتعين فيها تصريح بأداة تشريعية ( قانون) - وهي المتعلقة بالحقوق والحريات الشخصية - فانه يتعين بالنسبة لمعالجة البيانات الاسمية لحساب الدولة أو لحساب الهيئات العامة أو الهيئات المحلية أو الأشخاص المعنوية الخاصة والتي تقوم بإدارة خدمة عامة ، ان يتم تنظيم معالجة البيانات بلانحة بناء على موافقة من اللجنة القومية للمعلوماتية والحريات ، وإذا لم توافق اللجنة لم يكن من الممكن إصدار اللانحة إلا بناء على رأي من مجلس الدولة ، وإذا كان الأمر يتعلق بهيئة من الهيئات المحلية

(١) الشوابكة ، جرائم الحاسوب والانترنت ، مرجع سابق ، ص ٨٧ .  
(٢) د. آدم عبد البديع حسين ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، مرجع سابق، ص ٥٧٢ .

ولم توافق اللجنة لم يكن من الممكن إصدار اللائحة إلا بعد قرار من إدارتها يوافق عليه المجلس .

أما المادة ١٦ من ذات القانون - المشار إليه - فتتص على انه عندما يتعلق الأمر بمعالجة لخلاف الجهات المحددة بالمادة السابقة ، تعين أخطار اللجنة الوطنية للمعلوماتية والحريات قبيل إجراء معالجة البيانات ويجب ان ينطوي هذا الأخطار على إقرار بان المعالجة تتفق ومتطلبات القانون ، وعند استلام الجهة الطالبة ما يفيد العلم بوصول الأخطار للجنة ، فان بإمكانها البدء في معالجة البيانات علماً بان هذا لا يعفيها من مسؤوليتها<sup>(١)</sup> .

#### ثانياً : صور الركن المعنوي :

المعالجة الالكترونية للبيانات الشخصية دون ترخيص من اللجنة المختصة بذلك جريمة عمدية يتخذ ركن المعنوي صورة القصد الجنائي ويتحقق القصد الجنائي بتوافر عنصرين هما العلم والارادة ، اما العلم فيجب ان يشمل كل العناصر التي يتضمنها النموذج القانوني للجريمة فيلزم ان يعلم الجاني بالصفة الاسمية او الشخصية للبيانات وان يعلم ان من طبيعة الحاسوب اجراء المعالجة الالكترونية لهذه البيانات دون ترخيص من اللجنة المختصة بذلك ، ويتعين ايضاً ان تتجه الارادة لدى الجاني الى اجراء المعالجة الإلكترونية في اي صورة من صورها المختلفة ودون مراعاة للاجراءات الاولية التي نص عليها القانون<sup>(٢)</sup> .

أما صورة الخطأ فهي مستفادة من نص الشارع بالعقاب على إجراء المعالجة الآلية للبيانات الشخصية بدون ترخيص ، إذا كان ذلك نتيجة إهمال ورعونة الفاعل<sup>(٣)</sup> .

(١) الشوابكة ، مرجع سابق ، ص ٨٨

(٢) قايد ، مرجع سابق ، ص ٨٧ .

(٣) الشوابكة ، مرجع سابق ، ص ٨٩ .

### ثالثاً : العقوبة :

يعاقب المشرع الفرنسي على هذه الجريمة بعقوبة تتمثل بالحبس ثلاثة سنوات وغرامة خمسة واربعون الف يورو .

وقد كان أول الأحكام الصادرة عن القضاء الفرنسي فيما يتعلق بهذه الجريمة هو الحكم الصادر عن محكمة ( Nantes ) في ١٦ ديسمبر سنة ١٩٨٥ والتي قضت فيه بمعاقبة شخص بالحبس لمدة شهرين مع إيقاف التنفيذ وغرامة ٢٠.٠٠٠ فرنك وذلك للقيام بتسجيل بيانات خاصة دون إجراء أخطار مسبق إلى اللجنة المختصة بالإضافة بالاحتفاظ بهذه المعلومات<sup>(١)</sup> .

ونحن بصدد دراستنا لجريمة المعالجة الإلكترونية للبيانات دون ترخيص فان ثمة سؤالاً يثور في هذا الشأن هو ان :- هل يشكل فعل المعالجة الإلكترونية دون ترخيص تعدداً معنوياً للجرائم أم لا ؟ .

ذهب جانب من الفقه الفرنسي<sup>(٢)</sup> إلى ان فعل المعالجة دون ترخيص يعتبر تعدياً على الحرية الفردية ، ويخضع الفعل المكون لها لوصفين ، وصف الجريمة المنصوص عليها في المادة ( ٢٢٦ - ١٦ ) من قانون العقوبات الفرنسي الجديد المشار إليه سابقاً ، بالإضافة إلى وصف الجريمة المنصوص عليها في المادة ( ٤٣٢ - ٤ ) من ذات القانون<sup>(٣)</sup> مما يعد تعدداً معنوياً للجرائم .

(١) M . Pierre Sargos et – Michel masse "le droit penal special ne de "I informatiq  
Travaux de sciences criminelles de poitlers gujes. 1983 . p.36 نقلاً عن / آدم عبد البديع ،

مرجع سابق، ص ٥٧٥ .

(٢) M . Pierre Sargos et M .Michel masse – ibid . p. 36

نقلاً عن / آدم عبد البديع حسين ، المرجع نفسه ، صفحة ٥٧٤ .

ومن الفقه المصري :-

أ- د. محمد نجيب حسين ، شرح قانون العقوبات ، القسم العام الطبعة الخامسة ، دار النهضة العربية ،

القاهرة سنة ١٩٨٥ ، ص ٨٥٣

ب- د. مأمون سلامة ، قانون العقوبات، القسم العام الطبعة الرابعة ، دار الفكر العربي ، القاهرة سنة ١٩٨٤

، ص ٥٣١ .

(٣) تنص المادة (٤٣٢-٤) من قانون العقوبات الفرنسي الجديد على ان " كل شخص حائز على السلطة العمومية أو مكلف بمهمة في مصلحة عامة ، مارس في مزاولته عمله أو بمناسبة مزاولته لهذه المهام بأمور بأمور أو بفعله طريقة تعسفية عملاً ماساً بالحرية الشخصية ، يعاقب بسبع سنوات سجناً وسبعمئة ألف فرنك

وذهب فريق آخر من الفقه<sup>(٤)</sup> ، إلى ان فعل المعالجة الإلكترونية دون ترخيص للبيانات الشخصية لا ينطبق عليه إلا نص للمادة ( ٢٢٦-١٦ ) من قانون العقوبات الفرنسي وبالتالي فإن هذا الفعل لا يشكل تعددا معنويا للجرائم .

وبناءً على ما تقدم فإن وصف الجريمة المنصوص عليها في المادة ( ٢٢٦-١٦ ) هو الذي ينطبق على فعل المعالجة الإلكترونية دون ترخيص ، ولا ينطبق معه أي وصف آخر ، مما لا يعد بالتالي تعددا معنويا للجرائم .

وبالرغم من عدم وجود تشريع خاص لحماية المعلومات الشخصية في الاردن من اخطار بنوك المعلومات ، وخاصة فيما يتعلق بالتداول غير المرخص به للمعلومات فإنه يمكن الاستناد الى نص المادتين (٢٠،٢١) من قانون الاتصالات الاردني رقم (١٣) لسنة ١٩٩٥ وتعديلاته ، باعتبار ان شبكات الاتصال يمكنها ان تقدم معلومات مختلفة ، خاصة اذا تم ربط هذه الشبكات بالشبكات العالمية (الويب) ، وتم نقل وتبادل المعلومات عبر هذه الشبكات .

حيث تنص المادة (٢٠) على انه " لا يجوز انشاء شبكات عامة او تشغيلها او ادارتها او تقديم خدمة الاتصالات العامة الا بعد الحصول على ترخيص بذلك وفق احكام القانون " .

ونلاحظ من خلال النص ان المشرع الاردني قد اشترط لانشاء شبكات عامة أو تقديم خدمة الاتصالات العامة الحصول على رخصة من هيئة تنظيم قطاع الاتصالات ، وفق احكام القانون .

كما تنص المادة (٢١) من ذات القانون على " مع مراعاة احكام المادة (٢٢)<sup>(١)</sup> من هذا القانون يجوز انشاء شبكات الاتصالات الخاصة وتشغيلها دون الحصول على ترخيص بذلك من الهيئة باستثناء الترخيص اللازم لاستخدام الترددات الراديوية " .

فرنسي غرامه فإذا كان الفعل الماس بالحرية يشكل اعتقالا أو حجزا لمدة تزيد عن سبعة أيام تحول العقوبة إلى ثلاثين سنة سجنا وثلاثة ملايين فرنك غرامة " .  
(٤) Merle et Vitue Droit penel specile 1982 – Gujas. T. I NO 279. نقلاً عن / د. ادم عبد البديع حسين ، المرجع نفسه ، ص ٥٧٥ .

(١) تنص المادة (٢٢) على " يجوز للهيئة ان تصدر تعليمات تحدد بمقتضاها انواع الشبكات الخاصة والارشادات والشروط الفنية لانشائها وتشغيلها ، ويجوز للهيئة ان تشترط موافقتها على انشاء بعض انواع تلك الشبكات حسبما تقتضي الضرورة " .

ومن الجدير بالذكر ان المشرع في هذه المادة قد اجاز انشاء شبكات اتصال خاصة دون ترخيص ولكن ضمن شروط وإرشادات خاصة تناولته المادة ( ٢٢ ) . الا ان المشرع استثنى من ذلك الترددات الراديوية والزم من اراد انشاء هذه الشبكات الحصول على ترخيص من الهيئة ، باعتبار ان هذه الترددات تبث في الفضاء بصورة طبيعية ذات مدى معين .

## المطلب الثالث

### الإفشاء غير المشروع للمعلومات

عندما تخزن معلومات عن فرد معين، فانه يكون على يقين بان هذه المعلومات ستبقى أو يجب ان تبقى سرية ولا تستخدم إلا في الغرض المحدد لها ، ولا يمكن ان تكون مصدراً تعرضه للتشهير والى نشر ما لا يرغب ان يعرفه الآخرون عنه<sup>(١)</sup>

ولذلك فان الإفشاء غير المشروع للبيانات والمعلومات الشخصية المخزنة في بنوك المعلومات قد يضر بالفرد ويهدد مصالحه ويجعله في موضع حرج بالنسبة للآخرين ، مما يؤدي بالتالي إلى التشهير والإساءة إلى سمعته .

ان رضا الفرد في ان تخزن معلومات معينة عنه في بنوك المعلومات لدى جهة من الجهات التي تتولى الاشراف على مثل هذه البنوك يعني بالمقام الاول انه استودع سره لدى هذه الجهة ولن يضر منها بسبب ما لديها من معلومات عنها الا ان الامر يزداد خطورة عندما تقوم هذه الجهة بإفشاء هذه المعلومات الى الغير مما يؤدي الى اساءة استخدامها وانحرافها عن الغرض الذي جمعت من اجله ، فالفرد قد لا يرغب لنشر معلومات عنه حتى ولو كانت صحيحة اذ ان مجرد نشر معلومات من هذا النوع تكفي بالرغم من صحتها بان تجعله قضية تلوكها اللسن ويساء اليه من خلالها<sup>(٢)</sup> .

وفي رأينا فان معلومات الأفراد ليست آمنة من الاطلاع عليها وإفشائها من قبل الجهات الحكومية أو المؤسسات الخاصة ، وليست الخطورة فقط فيما يمكن الوصول إليه من معلومة في وقت معين ، إذ ان الخطر الأكبر فيما يمكن جمعه من معلومات وتحليلها كحزمة واحدة للوصول إلى حقائق عن الفرد تساهم في تنفيذ أنشطة المساس به أو الاعتداء على حقوقه الأخرى ، وبرز مثال في هذا الحقل ، قدرة أدماط من البرمجيات والنظم على تجميع عادات الشخص وحقائق معيشته على نحو قد يتيح في أي وقت الاعتداء على سمعته أو كرامته أو اعتباره المالي أو يساهم في توفير فرصة

(١) مغيب ، مخاطر المعلوماتية والانترنت ، مرجع سابق ، ص ٢٤٤ - ٢٤٥ .

(٢) Simitis ,Spiros: "Reviewing Privacy in an Information Society" Yniversity of Pennsylvania Law Riview, Vol,1986,P . 710-711

نقلا عن / المقاطع ، مرجع سابق ، ص ١٠٢

حقيقية لاختراق نظامه واستخدام بياناته السرية للوصول إلى حساباته البنكية ومباشرة أفعال اعتداء مختلفة عليها .

واليوم وفي ظل التطور العلمي والتكنولوجي فان "الإنسان المعاصر قد يفاجأ في أحوال كثيرة وبمناسبات مختلفة بحوادث معينة تسيء إلى سمعته وتشهّر به دون ان يكون هو مستعداً لها، وما كان ذلك ليحدث لولا سهولة الوصول للمعلومات الخاصة به، والمخزنة في بنوك المعلومات لأغراض وبأشكال وأماكن مختلفة" (١) .

ومن الجدير بالذكر أن الدول في الأنظمة القانونية المختلفة لم تسلك مسلكاً موحداً لحماية المعلومات الشخصية للأفراد في مواجهة الأخطار الناجمة عن استخدام بنوك المعلومات ، بل تباينت مواقفها في هذا الشأن ، وفيما يلي بيان لموقف التشريع الفرنسي والتشريع الأمريكي كنموذجين لنظامين قانونيين مختلفين هما النظام اللاتيني والنظام الانجلو أمريكي لما لهما من قيمة قانونية وتشريعية تتمثل في تقدمهما في علاج المشاكل والأخطار الناجمة عن استخدام بنوك المعلومات التي حملت في طياتها تهديداً للمعلومات الشخصية للأفراد ولحياتهم الخاصة ، وذلك من خلال الإفشاء غير المشروع للمعلومات الشخصية للأفراد والتشهير والإساءة الى السمعة كطريق من طرق الاعتداء على هذه المعلومات ، ثم نعرض أخيراً لموقف تشريعنا الأردني من هذه الأخطار وذلك في ثلاثة فروع وعلى النحو الآتي :-

## الفرع الأول

موقف التشريع الفرنسي من الإفشاء غير المشروع للمعلومات الشخصية

اصدر المشرع الفرنسي القانون رقم ١٧ لسنة ١٩٨٧ والخاص بالمعالجة الإلكترونية للبيانات الاسمية ، والذي اشتهر باسم قانون معالجة المعلومات والحريات ، والذي بينت المادة الأولى منه أن معالجة المعلومات يجب ان تكون في خدمة كل مواطن .

(١) المرجع السابق ، ص ١٠٣



وقد دعم المشرع الفرنسي هذا المبدأ بوضع عدة قوانين راعى فيها التطور التكنولوجي، لكن ما يهمنا هنا هو قانون العقوبات لعام ١٩٩٢ والمعمول به منذ عام ١٩٩٤ ، حيث نص على جريمة الإفشاء غير المشروع للبيانات الاسمية في المادة (٢٢٦-٢٢٢) من هذا القانون بقولها " يعاقب بالحبس سنة وغرامة خمسة عشر الف يورو كل شخص كان قد استقبل أو (تلقى) بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الإلكترونية ، بيانات اسمية من شأن إفشائها الأضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة ، وقام بنقلها إلى من لا حق له في العلم بها ، وإذا وقع هذا الإفشاء للبيانات الاسمية بطريق الإهمال تكون العقوبة هي الغرامة سبعة الاف وخمسة يورو ، ولا تسري الدعوى العمومية وفقاً للفقرتين السابقتين الإشارة إليهما ، إلا من خلال شكوى المجني عليه أو ممثله القانوني ، أو من له صفة في ذلك" (١).

ونتناول بالعرض للركن المادي وللركن المعنوي لهذه الجريمة ثم للعقوبة المقررة لها ، وذلك كون المشرع قد نص على هذه الجريمة صراحة وأسبغ حمايته للبيانات الشخصية في حالة الإفشاء غير المشروع لها .

#### أولاً : الركن المادي :

يتحقق النشاط المادي لهذه الجريمة بتوافر صورتين :-

الصورة الأولى : فعل الحيازة للبيانات الاسمية ، ويستوي ان تكون حيازة البيانات الاسمية بقصد تصنيفها أو نقلها أو علاجها تحت أي شكل ، فيجب بداية ثبوت واقعة حيازة الجاني لهذه البيانات الشخصية للقيام بأي إجراء من الاجراءات السابقة (٢) حتى يتسنى له تصنيف هذه البيانات او نقلها او علاجها .

(١) أحالت المادة إلى هذا النص المادة(٤٣) من قانون العقوبات الفرنسي القديم ( ٦ يناير ١٩٧٨ ) والتي تنص على ان " يعاقب بالحبس من شهرين إلى ستة اشهر وبالغرامة من ألفين إلى عشرين ألف فرنك أو بإحدى العقوبتين كل من حاز بمناسبة تسجيله أو تصنيفه أو نقله لأي شكل للعلاج الإلكتروني بيانات اسمية يشكل إفشاؤها اعتداء على الشرف أو الاعتبار أو حرمة الحياة الخاصة ، دون تصريح من صاحب الشأن ، أو ينقل عمداً إلى علم شخص غير مختص بتلقي هذه البيانات وفقاً للأحكام المنصوص عليها في القانون ، وعاقب كل شخص بالغرامة من ألفي فرنك إلى عشرين ألف فرنك إذا وقعت الجريمة نتيجة رعونة أو إهمال أو ترك بيانات من ذات الطبيعة المنصوص عليها في الفقرة الأولى " .

(٢) قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، مرجع سابق ، ص ٩٣ .

الصورة الثانية :- فعل إفشاء البيانات للغير الذي لا يكون من حقه الاطلاع عليها، فإذا كان فعل الإفشاء لشخص من حقه الاطلاع على هذه البيانات ، فان النشاط المادي لا يعد متوافراً وبالتالي لا تتحقق الجريمة<sup>(٣)</sup> .

ويتطلب المشرع الفرنسي لقيام الركن المادي توافر ثلاثة شروط هي :-

١. ان يكون من طبيعة فعل الإفشاء ان يضر بالمجني عليه ، وذلك باقتران فعل الإفشاء بالاعتداء على الاعتبار أو الحياة الخاصة للفرد ، ولا يشترط ان تكون مصادر هذه البيانات صحيحة لكي يتحقق الاعتداء ، فيستوي ان تكون صحيحة أو غير صحيحة في نظر القانون ، أو ان تكون مصادر هذه البيانات لا تدخل بطبيعتها أي اعتداء على الحياة الخاصة أو الشرف أو الاعتبار ، ما دام ان إفشاء هذه البيانات يحقق هذا الاعتداء<sup>(١)</sup> .

٢. ان يكون إفشاء البيانات بدون رضاء المجني عليه صاحب العلاقة ، وبالتالي لا تتحقق هذه الجريمة إذا كان الإفشاء قد تم بناءً على موافقة صاحب الشأن الصريحة .

٣. ينبغي ان يكون الإفشاء إلى شخص ليس له حق الاطلاع على هذه البيانات. وقد أوضح مجلس الدولة الفرنسي هذا الشرط بقوله ، ان البيانات التي يجمعها البوليس عن الأشخاص من اجل حماية الأمن العام ، ويقاء هذه البيانات تحت سلطة هؤلاء الموظفين بسبب وظيفتهم في حماية الأمن العام - وهي أساس علمهم بهذه البيانات - ومن ثم يجب منع غيرهم من الوصول إليها ممن ليس لهم نفس الاختصاص<sup>(٢)</sup> .

ثانياً :- الركن المعنوي :-

يأخذ الركن المعنوي لجريمة الإفشاء غير المشروع للبيانات الاسمية صورة العمد أو الخطأ.

(٣) الشوابكة ، جرائم الحاسوب والانترنت ، مرجع سابق ، ص ١٠٢ .  
(١) د. آدم عبد البديع ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، مرجع سابق ، ص ٥٨١ .  
(٢) د. أسامة عبد الله قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، مرجع سابق ، ص ٩٣ ، ٩٤ .

وتتحقق صورة العمد بتوافر القصد الجنائي العام ، والذي يقوم بتوافر العلم والإرادة، فيتعين ان يكون الجاني عالماً بأنه يقوم بإفشاء بيانات اسمية تشكل اعتداء على الاعتبار أو الحياة الخاصة للأفراد ، ويتعين كذلك ان تتجه إرادته نحو تحقيق ذلك<sup>(٣)</sup> .

وتتحقق صورة الخطأ إذا كان فعل الإفشاء للغير قد وقع نتيجة إهمال أو رعونة أو ترك للبيانات الاسمية .

### ثالثاً :- العقوبة :

فرق المشرع في العقاب على هذه الجريمة على أساس الركن المعنوي ، فنص على عقوبة مشددة في حالة الإفشاء العمد ، دون حالة الإفشاء في صورته غير العمدية ، فنص في الحالة الأولى على عقاب الجاني بالحبس سنة والغرامة سبعة الاف وخمسمائة يورو ، أما في الحالة الثانية فقد اقتصر المشرع على عقوبة الغرامة فقط والتي مقدارها خمسون ألف فرنك فرنسي.

هذا ، وقد نص الشارع على سبب لإباحة فعل الإفشاء للبيانات الاسمية ، هو رضاء المجني عليه ، والعلة في اعتبار رضاء المجني سبباً للإباحة ، ان هذا الرضاء يزيل عن الفعل صفة الاعتداء ، ومن ثم ينفي عنه الصفة غير المشروعة<sup>(١)</sup> .

## الفرع الثاني

موقف التشريع الأمريكي من الإفشاء غير المشروع للمعلومات الشخصية

من المعلوم ان المشرع الأمريكي لم يحم البيانات الخاصة للأفراد التي تتعلق بالخصوصية بنصوص مباشرة ولكن بطريقة غير مباشرة عن طريق النصوص العامة

(٣) المرجع نفسه ، ص ٩٤

(١) د . أسامة عبد الله قايد ، المسؤولية الجنائية للطبيب عن إفشاء سر المهنة ، بدون طبعة ، دار النهضة العربية ، القاهرة ، ١٩٨٧ ، ص ٧٢ .

بحماية خصوصية الفرد وحماية المعلومات ، خلافاً للمشرع الفرنسي الذي وضع قانوناً خاصاً لحماية الحياة الخاصة والحريات في مواجهة المعالجة الالكترونية للبيانات . ولذا فإنه لم تكن هناك جريمة إفشاء غير مشروع بالمعنى المنصوص عليه في القانون الفرنسي ، حتى نتعرض لها بالتفصيل ، ولكن في هذا المقام سوف تتم الإشارة إلى بعض التشريعات التي عالجت حماية البيانات الشخصية من مخاطر الاعتداء عليها ، ونعرض لها على النحو التالي :-

١. كان أول تشريع وضعه المشرع الأمريكي في سنة ١٩٧٠ لحماية البيانات وحق الوصول إليها لتصحيح البيانات غير الصحيحة .
٢. تم إصدار قانون خاص لحماية المعلومات الشخصية في عام ١٩٧٤ وكان الهدف منه حماية هذه المعلومات وصيانتها من عبث السجلات الفدرالية . ويعد هذا القانون من التشريعات المتقدمة في حماية الحياة الخاصة للأفراد من إفشاء المعلومات الخاصة بهم ، والذي يهدف الى تقرير حماية لكل فرد ضد الاعتداء على حياته الخاصة ووضع قواعد لحماية الفرد من الاطلاع على المعلومات الخاصة به والمحافظة في الكمبيوتر<sup>(٢)</sup> .

فقد نصت المادة (٥٥٢/أ) منه على انه لا يجوز لأي جهة ان تفشي أي معلومات يتضمنها نظام للمعلومات بأي وسيلة من الوسائل لأي شخص أو لأي جهة أخرى ما لم يكن ذلك بناءً على طلب كتابي بموافقة صاحب الشأن الذي تتعلق به المعلومات ، مع إيراد استثناء يتعلق بالمصلحة العامة أو بناء على أمر المحكمة<sup>(١)</sup> .

وكذلك يعاقب قانون ولاية ( فلوريدا ) على كل ولوج بسوء نية في نظام أو شبكة معلوماتية بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير ، أو كل من ادخل معلومات مصطنعة بغرض تحسين أو إساءة سمعة الغير<sup>(٢)</sup> .

(١) طارق احمد فتحي سرور : الحماية الجنائية لأسرار الأفراد في مواجهة النشر ، رسالة مقدمة للحصول على درجة الماجستير في الحقوق ، كلية الحقوق ، جامعة القاهرة ، ١٩٩١ ، ص ١٥٩ .

(٢) نقلاً عن / أسامة احمد المناعسة ، جرائم الحاسب الآلي والانترنت ، دراسة تحليلية مقارنة ، الطبعة الأولى ، دار وائل للنشر ، الأردن ، ٢٠٠١ ، ص ٢٢٣ .

(٣) المرجع نفسه ، ص ٢٢٤ .

## الفرع الثالث

### موقف التشريع الأردني من الإفشاء غير المشروع للمعلومات الشخصية

تعتبر الأردن من الدول النامية التي التزمت الصمت نحو أخطار بنوك المعلومات على الحياة الخاصة بشكل عام ، وقد اكتفى التشريع الأردني بالنصوص الخاصة بحماية الأسرار، ولكن عند استقراء نصوص التشريعات الجزائية الخاصة بحماية الحق في حرمة الحياة الخاصة ، وكذلك نصوص التشريعات الخاصة بحماية البيانات ، لم نجد بينها ما يكفل حماية هذا الحق في مواجهة الأخطار الناجمة عن استخدام الحاسبات الالكترونية كبنوك للمعلومات ، وفيما يلي عرض موجز لهذه النصوص حتى يتبين لنا مدى الحاجة لوضع تشريع خاص لحماية البيانات الشخصية التي تتعلق بالحياة الخاصة للأفراد وذلك على النحو الذي انتهجته غالبية الدول المتقدمة .

أولاً :- النصوص الجزائية التي تتعلق بإفشاء الأسرار:

عند استقراء نصوص قانون العقوبات الأردني لم نجد نصاً واحداً يجرم الإفشاء غير المشروع للبيانات والمعلومات الشخصية على غرار ما هو موجود في قانون العقوبات الفرنسي مثلاً ، إلا ان نص المادة (٣٥٥) <sup>(٣)</sup> والمتعلقة بإفشاء الأسرار الرسمية قد جرمت لمن أباح هذه الأسرار بحكم وظيفته واطلع الغير الذي ليس له صلاحية الاطلاع عليها .

(٣) المادة (٣٥٥) " يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من -

١. حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية وأباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقاً للمصلحة العامة.
٢. كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسوماً أو مخططات أو نماذج أو نسخاً منها دون ان يكون له حق الاحتفاظ بها أو دون ان تقتضي ذلك طبيعة وظيفته .
٣. كان بحكم وظيفته على علم بسر وأفشاء دون سبب مشروع .

وإذا كانت هذه المادة تعاقب على " جريمة إفشاء الأسرار " فإن التساؤل يثور حول مدى صلاحية تطبيقها على حالة إفشاء المعلومات الشخصية التي يتم معالجتها إلكترونياً وتخزين في بنوك المعلومات ؟ .

يرى احد الفقه ان محل جريمة افشاء الاسرار المنظمة بقانون العقوبات الاردني تكون اما اسراراً رسمية او اسراراً مرتبطة ببعض المهن المؤتمنة التي تفترض الثقة كمحور اساسي لها ( كمهنة الطب او المحاماة او تدقيق الحسابات ، ... الخ ) الامر الذي يترتب عليه القول انها بهذا المعنى تختلف عن افشاء البيانات الاسمية التي محلها البيانات الشخصية المعالجة آلياً بنظام الحاسوب<sup>(١)</sup> . ويخلص هذا الرأي الى ان النصوص العقابية الخاصة بجريمة افشاء الاسرار لا تصلح لحماية البيانات الاسمية التي تكون محلاً للمعالجة الالية ، برغم الاتفاق فيما بينهما في العلة التشريعية والمتمثلة في ( حماية البيانات والمعلومات المتعلقة بالاشخاص الطبيعيين ) ، الا انها تخلفان في الموضوع والمحل<sup>(٢)</sup> .

ووفقاً لما هو مستقر عليه في الفقه والقضاء<sup>(٣)</sup> ، وتأكيداً لمبدأ الشرعية الجنائية ، انه لا يجوز القياس في تفسير نصوص التجريم والعقاب ، فلا يجوز للقاضي الجنائي ان يقيس فعلاً لم يرد في شأنه نص تجريم في قانون العقوبات على فعل يرد نص بتجريمة ، فيقرر للفعل الأول عقوبة الثاني محتجاً بتشابه الفعلين أو أن العقاب على الثاني يحقق نفس المصلحة التي يحققها العقاب على الأول . وبناءً على ذلك فإنه لا يجوز قياس البيانات أو المعلومات الشخصية التي يتم معالجتها بواسطة أجهزة الحاسبات الإلكترونية ثم تحفظ في بنوك المعلومات على البيانات الخاصة بتعداد السكان مثلاً في حالة جمعها أو إفشائها أو إساءة استخدامها .

(١) الشوابكة ، جرائم الحاسوب والانترنت ، مرجع سابق ، ص ٦٠ .  
(٢) د. نائل عبد الرحمن صالح ، واقع جرائم الحاسوب في التشريع الجزائي الأردني ، مرجع سابق ، ص ١٠ .  
(٣) د. جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الكتاب الاول ، "الجرائم الناشئة عن الحاسب الالي " ، الطبعة الاولى ، دار النهضة العربية ، القاهرة ، ١٩٩٢ ، ص ٢١ .  
وكذلك د. محمد صبحي نجم ، شرح قانون العقوبات الاردني ، القسم العام ، الطبعة الثانية ، دار الثقافة ، عمان ، ١٩٩١ ، ص ٦٧ .

## ثانياً : النصوص الخاصة بحماية البيانات :

لم يحم المشرع إلا البيانات التي تجمع بشأن التعداد والإحصاءات ، فنص في المادة ( ١١ ) من قانون الإحصاءات العامة الأردني<sup>(١)</sup> على سرية البيانات الفردية التي تتعلق بأي إحصاء أو تعداد، لا يجوز اطلاع أي فرد أو هيئة عامة أو خاصة عليها أو إبلاغ شيء منها ، أو الكشف عنها ، كما لا يجوز استخدامها لغير الأغراض الإحصائية أو نشر ما يتعلق منها بالأفراد كما ألزم المشرع الدائرة باتخاذ كافة الاحتياطات اللازمة لحماية البيانات التي يتم جمعها وحفظها في أماكن تتوافر فيها شروط السلامة والأمان .

وشدد المشرع العقاب في حالة إفشاء هذه البيانات أو استخدام وسائل غير مشروعة في الحصول عليها ، فنص في المادة ( ١٥ ) من هذا القانون على : أ. يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن خمسمائة دينار ولا تزيد على ألف دينار او بكلتا العقوبتين أي من موظفي الدائرة إذا ارتكب أيًا من الأفعال التالية :

١. إفشاء أي معلومات أو بيانات إحصائية سرية بالمعنى المنصوص عليه في المادة ( ١١ ) من هذا القانون أو سر من أسرار الصناعة أو التجارة وغير ذلك من أساليب العمل التي تعتبر من أسراره ويكون قد اطلع عليها بحكم عمله .
٢. تعمد الاحتفاظ بأي وثائق إحصائية تحتوي على البيانات أو تعمد إتلافها أو تزويرها .
٣. إضاعة أي وثائق إحصائية لها صفة سرية تحتوي على البيانات بسبب الإهمال .

(١) المادة (١١) من قانون الإحصاءات العامة الأردني المؤقت رقم ٨ لسنة ٢٠٠٣ تنص على :  
أ. تعتبر سرية جميع المعلومات والبيانات الفردية التي تقدم للدائرة والمتعلقة بأي مسح أو تعداد ولا يجوز لها أو لأي من العاملين لديها ، تحت طائلة المسؤولية القانونية ، اطلاع أي شخص أو جهة عامة أو خاصة عليها أو الكشف عنها كلياً أو جزئياً ، أو استخدامها لأي غرض غير اعداد الجداول الإحصائية .  
ب. تنقيد الدائرة عند نشرها للإحصاءات الرسمية بعدم اظهار أي بيانات فردية حفاظاً على سريتها .  
ج. يتعين على كل موظف في الدائرة اداء القسم والتوقيع على تعهد يلتزم بموجبه بعدم إفشاء أو نشر أي معلومات أو بيانات فردية .  
د. على الدائرة اتخاذ الإجراءات الكفيلة بحماية البيانات التي يتم جمعها وحفظها في أماكن تتوافر فيها شروط الأمان والسلامة .

ب. يعاقب بالحد الأعلى للعقوبة الواردة في الفقرة (أ) من هذه المادة أي من موظفي الدائرة في حال تكرار أي من الأفعال المذكورة فيها .  
كما ان قانون المعاملات الالكترونية الأردني المؤقت رقم (٥٨) لسنة ٢٠٠١ وفي المادة (٣٧)<sup>(١)</sup> منه تحديداً قد عاقب أي جهة تمارس أعمال توثيق المستندات ، اذا قامت بتقديم معلومات غير صحيحة في طلب التسجيل ، أو أفشت أسرار احد العملاء.

اما فيما يتعلق بقانون ضمان حق الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧ فان المشرع الاردني لم يعالج فيه طرق الاعتداء على المعلومات الشخصية مثل التداول غير المرخص به للمعلومات او الافشاء غير المشروع للبيانات الشخصية ، وهذا يعتبر قصور في هذا التشريع ، نتمنى ان يتم تداركه من قبل المشرع ، حيث اننا لم نجد نصاً واحداً يجرم مثل هذه الامور ، والتي يمكن من خلالها ان يتم الاعتداء على خصوصية المعلومات الشخصية للأفراد .

ومؤدى هذه النصوص في رأينا ان المشرع قصر الحماية على البيانات الفردية التي تقتضي إجراء إحصاء سكاني او تعداد ، وهذه البيانات لا تخرج عن كونها بيانات خاصة بالحالة الجنائية والصحية والاجتماعية للأفراد او اتجاهاتهم السياسية ، والتي تخزن عادة في بنوك المعلومات ولا يصح القول بأن هذه النصوص يمكن تطبيقها فيما يتعلق ببنوك المعلومات سواء الخاصة بالمنشآت الخاصة بشركات التأمين او البنوك ، او العامة كالوزارات والهيئات الحكومية التي تتضمن بيانات عن الحياة الخاصة للأفراد، او عن مختلف النواحي الاقتصادية والاجتماعية للأفراد لتعلقها بالإحصاء او التعداد وفقاً لصريح نص المشرع .

ومن خلال مقارنة النصوص الخاصة بحماية البيانات التي تجمع بشأن الإحصاء والتعداد السكاني ، نلاحظ ان المشرع الاردني كان اكثر تشدداً من المشرع الفرنسي بخصوص هذه المسألة .

(١) المادة (٣٧) تعاقب أي جهة تمارس أعمال توثيق المستندات بغرامة لا تقل عن (٥٠٠.٠٠٠)دينار إذا قامت بتقديم معلومات غير صحيحة في طلب التسجيل أو أفشت أسرار أحد عملائها أو خالفت الأنظمة والتعليمات التي تصدر استناداً إلى هذا القانون .





## المطلب الرابع

### الأخطاء في المعلومات والبيانات

عندما تؤخذ المعلومات عن فرد معين فإنها تخزن آليا في بنوك المعلومات ، وبالتالي فإنها دون شك عرضة لجملة من الأخطاء الفنية من ناحية والأخطاء البشرية من ناحية أخرى .

فالأخطاء الفنية هي التي قد تحدث من جهاز الحاسوب نفسه والتي يكون مرجعها إلى عيب فني في الجهاز أو اختلال في الضغط الكهربائي ، الأمر الذي يترتب عليه دمج البيانات المختلفة، أو اختلال في تصنيفها وتنظيمها أو محو تسجيلها ، مما ينتج عنه نسبة معلومات معينة لأشخاص لا تتعلق بهم ، ويعطي صورة غير حقيقية عن حالتهم الاجتماعية أو وضعهم الحقيقي من الناحية المالية أو السياسية أو المهنية أو الصحية ، مما يعد تهديداً خطيراً لحياة الفرد في خصوصية معلوماته .

أما الخطأ البشري فهو يقع عادة من الأشخاص الدانمين بعمليات التجميع أو التخزين للبيانات أو ترتيبها أو تصنيفها ، فقد يحدث خطأ في أي مرحلة من المراحل السابقة مما ينتج عنه دمج بيانات مختلفة عن أشخاص مختلفين وخروج معلومات غير دقيقة وغير صحيحة عن كل منهم ، ولا سيما ان أصحاب هذه البيانات في اغلب الأحيان لا يكونوا حاضرين وقت إجراء هذه العمليات والتأكد من صحة البيانات .

إلا ان الأمر الذي نود ان نقرره هنا هو بان مجرد وجود خطأ ( تقني أو بشري ) في المعلومات المخزنة عن الفرد آليا ستترك أثارا سلبية على حياته الخاصة وسيرته لدى كل من يطلع على هذه البيانات والمعلومات ، مما يؤدي إلى انتهاك حقه في الخصوصية ، والحاق الضرر به ويجعله في وضع خاطئ يؤدي إلى ازدياد الناس له أو سوء تعاملهم معه .

ولكن الواقع العملي يكشف لنا عن حقيقة هامة هي ان أهم المشاكل التي يواجهها من لديهم ملفات اشتباه اليوم ، مخزنة آليا ، هو عدم قدرتهم على التحكم بها ، وهي تحتوي على معلومات غير كاملة أو غير دقيقة عنهم أو خاطئة ، وهو ما يرتب

النظرة السيئة لهم من قبل الآخرين ، بل وحتى لدى زملائهم في العمل وأرباب العمل ، مما قد يؤثر على أداء الانسان الطبيعي في حياته اليومية<sup>(١)</sup> .

وتشير الدراسات في حقل المعلوماتية بان الأخطاء التي تقع في الحاسبات المرتبطة ببنوك المعلومات كبيرة ومتعددة ، وهو ما أكدته شركات الكمبيوتر ذاتها ، والتخوف هنا هو ان يكون الخطأ مؤثراً بشكل كبير على حقوق ومصالح الأفراد من وقت وقوعه إلى حين اكتشافه ، والخطورة أيضاً تتمثل في حالة اتصال الحاسب كبنك للمعلومات بمؤسسات تجارية أو شركات صحية ، مثل شركات الضمان أو مؤسسات إصدار بطاقات الائتمان ، والذي قد يؤدي وجود مثل هذه الأخطاء في المعلومات التي لديها إلى قيام هذه المؤسسات برفض تمتع شخص بخدماتها بسبب وجود خطأ من هذا النوع في ملفه<sup>(١)</sup> .

وتزداد الخطورة أيضاً إذا تمت معالجة البيانات من اجل استخلاص حكم أو تقييم للشخصية من دافع ما غذي به الحاسب الآلي من معلومات فالتوصل إلى نتائج انطلاقاً من البيانات المتفرقة الخاطئة يهدد باستخلاص نتائج غير دقيقة سواء من حيث سلوكه أو صفاته أو سمعته ، مما يؤدي إلى تلويث شخصيته . فمن اخطر ما يهدد الانسان هو استخلاص أحكام قيمية على أساس بيانات دون دراسة شخصية الانسان نفسه محل التقويم<sup>(٢)</sup> .

ويمكن ان يتم استخدام البيانات والمعلومات الشخصية بطريقة غير صحيحة ، مما يؤدي بالنتيجة إلى افتئات واعتداء على خصوصية الفرد ، ويتحقق هذه الانتهاك المعلوماتي للخصوصية في صورتين هما :-

١ . التلاعب في البيانات الشخصية أو محوها من قبل أشخاص غير مرخص

لهم :

(١) المقاطع ، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ١٠١ .

(١) Raymond Walks "The Protection of Privacy" , Sweet & Maxwell Limited , London , 1980 , P .124

نقلاً عن / المقاطع ، مرجع سابق ، ص ١٠١

(٢) نعيم عطية ، حق الأفراد في حياتهم الخاصة ، مجلة إدارة قضايا الحكومة ، العدد الرابع ، السنة الحادية والعشرين ، ص ٨٧ .

ويقترن هذا التلاعب أو المحو عادة بتحقيق مصالح مالية للجناة ، بجانب انتهاكه  
للديرية، وحرمة خصوصيات الأفراد . ومن أمثاته الواقعية يمكن ان نشير إلى حالة  
شركة T R W Company Credit Data الأمريكية .

وتتلخص وقائع هذه الحالة (٣) في ان " الشركة كانت تزود عملائها ، وأكثرهم من  
البنوك والمتاجر الكبرى وشركات تسهيلات الائتمان وشركات تأجير السيارات والمعدات  
الثقيلة ، من خلال حساباتها وانظمتها المعلوماتية بمعلومات تتعلق بالمركز الائتماني  
لأفراد الجمهور نظير اشتراك يدفعه العملاء ، وتقدم بذلك لعملائها المشتركين في هذه  
الخدمة النصيحة بشأن مخاطر المركز الائتماني الرديء لمن يتعامل أو يرغب في  
التعامل معهم ، وذلك من واقع بيانات عن أشخاص (بلغ عددهم سنة ١٩٧٦ حوالي  
خمس مليون شخص ) كانت الشركة تقوم بجمعها وحفظها في الملفات المخزنة لدى  
حساباتها" .

وقد أغرى هذا النشاط ستة من العاملين بالشركة من بينهم كاتب بقسم علاقات  
المستهلكين على الاتجار بهذا النشاط "ببيع" مراكز ائتمانية جيدة ، يتم اختلاقتها  
لاصحاب المراكز الائتمانية الرديئة مقابل مبلغ من المال يتفق عليه ، وبحيث يتم تعديل  
أو محو المراكز الثانية من ملفات الحاسب لتحل الأولى محلها . وفي تنفيذ عملياتهم  
استغل الجناة الأسماء والعناوين وسائر البيانات المفصلة المسجلة عن الأشخاص في  
الملفات المخزنة بحاسب الشركة في الاتصال بأصحاب المراكز الائتمانية الرديئة  
عارضين عليهم إحلال سجل ائتماني نظيف محل سجلاتهم الرديئة الموجودة في ملفات  
الحاسب ، ومن يبدي موافقته على العرض يدفع المبلغ الذي يحدده الجناة مقابل هذه  
الخدمة ، كان يقوم بتزويدهم بما يراه ملائماً من بيانات تحقق هدفه في تحسين بيانات  
سجله الائتماني ، فيقوم موظف قسم علاقات المستهلكين بإدخال هذه البيانات المزورة  
إلى نظام معلومات حاسب الشركة ، وبطبيعة الحال ، فقد كان لازماً ، في بعض الأحيان  
، إزالة أو حذف بيانات تسيء إلى مركز الشخص الائتماني من الملفات ، وفي أحيان  
أخرى كان لازماً بعد المحو إضافة بيانات من شأنها تحسين هذا المركز(١) .

وبناءً على البيانات الائتمانية الزائفة التي تم إدخالها ، بالمحو أو الإضافة أو  
بهما معاً إلى نظام معلومات حاسب شركة (TRW) تورط العديد من عملائها في

(٣) نقلاً عن / رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مرجع سابق ، ص ١٨٧-١٨٨ .  
(١) رستم ، مرجع سابق ، ص ١٨٨ .

معاملات مالية وتجارية مع أشخاص ذوي سمعة انتمائية سيئة ، وقد قدر عدد السجلات التي تم التلاعب في بياناتها بأكثر من مائة سجل ، رغم ان الادعاء العام اقتصر على تسجيل ست عشر حالة تزوير فقط .

٢. جمع أو معالجة أو نشر بيانات شخصية غير صحيحة من قبل المرخص لهم بذلك قانوناً :

قد تنصب أفعال الجمع أو المعالجة أو النشر التي يأتيها المرخص لهم بذلك قانوناً على بيانات مزورة أو غير صحيحة ، ومع ان ارتكاب هذه الأفعال قد يكون مصحوباً بالعلم بمخالفة البيانات الشخصية للحقيقة ، إلا ان ذلك لا يحدث عادة في مجال المعالجة الإلكترونية للبيانات ، وبوجه خاص في نطاق نظم تقارير الائتمان حيث يكاد الإهمال ان يكون السبب الوحيد تقريباً ، لجمع ومعالجة ونشر بيانات غير صحيحة (١) .

وترتيباً لما تقدم وحتى لا يضر الفرد ويفقد حقه في خصوصية معلوماته ، فان العديد من الدول قد سعت من اجل ضمان حق الفرد بان لا تعطى معلومات ناقصة أو خاطئة عنه ، ومن ذلك مثلاً ما عمدت إليه الولايات المتحدة الأمريكية في قانون أصدرته عام ١٩٨٨ ينظم عملية تبادل المعلومات ، حيث فرض هذا القانون على كل جهاز حكومي قبل ان يكشف عن أية معلومات لأي جهة من الجهات ، ان يقوم بتمحيص ما لديه من بيانات ليؤكد بان جميع المعلومات التي كانت أو ستكون محلاً لبرامج تبادل معلومات صحيحة (٢) .

ان خطورة المعلومات الخاطئة تكمن ، في اعتماد الأجهزة الحكومية والمؤسسات الخاصة والشركات عليها ، وعلى الأخص عند استقائها من بنوك المعلومات بل وتعامل على انها معلومات مسلم بصحتها ، وهو الأمر الذي يرتب نتائج خطيرة إذا ما اتخذت أي قرارات استناداً لمثل تلك المعلومات ، مما يضر معه الفرد ويفقد حقه في خصوصية معلوماته وقدرته في السيطرة عليها (٣) .

وفي رأينا فان الفرد قد يضر في حقه في الخصوصية نتيجة نسبه معلومات خاطئة أو غير صحيحة إليه مما يرتب نتائج وخيمة شأنها ان تضر بمصالح الأفراد

(١) رستم ، مرجع سابق ، ص ١٨٨ .  
(٢) المقاطع ، حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ١٠٢ .

(٣) المرجع نفسه ، ص ١٠٢ .

وتهدد خصوصياتهم، وتعرضهم إلى استهجان وازدراء الآخرين ، الأمر الذي يستدعي من الجهات القائمة على بنوك المعلومات اخذ كافة الاحتياطات اللازمة وتوخي الدقة عند قيامها بجمع أو تخزين وحفظ المعلومات عن الأفراد ، لان أي خطأ فني من الآلة نفسها سواء في عملها أو في وضع البرامج ، مما قد يكون له أسوأ الأثر في استخلاص نتائج معينة عن الحياة الخاصة للشخص ، كما ان أي خطأ بشري يقع من الأشخاص العاملين على بنوك المعلومات ، قد ينسب معلومات معينة إلى شخص آخر ، مما يهدد مصالحه ويلحق الضرر به نتيجة هذه المعلومات الخاطئة ، وقد يقع الاعتداء نتيجة إفشاء بعض المعلومات من الأشخاص العاملين أنفسهم .

من هنا فان غالبية الدول المتقدمة علمياً وتكنولوجياً ، قد تنبعت إلى خطورة بنوك المعلومات على خصوصيات الأفراد ، الأمر الذي تطلب من هذه الدول إصدار التشريعات الخاصة لحماية المعلومات الشخصية للأفراد من أخطار التكنولوجيا الحديثة ، كضمانة أساسية لحق الفرد في خصوصية معلوماته في مواجهة أي إعتداء أو إفتئات على حقه في الخصوصية .

وهذا ما سوف نعالجه في الفصل الثاني من هذه الدراسة .

## الفصل الثاني

### مبادئ حماية المعلومات الشخصية وضماناتها

#### في مجال تجميعها في بنوك المعلومات

#### تمهيد وتقسيم :-

تعتبر الخصوصية أحد حقوق الإنسان الرئيسية ، التي تتعلق بكرامة الفرد وبقيم مادية ومعنوية أخرى كالحق في الرأي والحق في التعبير والمشاركة السياسية ، وقد اصبح الحق في الخصوصية واحداً من أهم حقوق الإنسان في العصر الحديث . وجرى الاعتراف بالخصوصية ضمن ثقافات ونظم غالبية الدول ، فجرى حمايتها في الإعلان العالمي<sup>(١)</sup> لحقوق الانسان وفي العهد الدولي<sup>(٢)</sup> للحقوق المدنية والسياسية ، وفي غالبية اتفاقيات<sup>(٣)</sup> حقوق الإنسان الدولية والإقليمية ، وتقريباً فان كل دولة في العالم ضمنت دستوراً حكماً بشأن الخصوصية، في حدها الأدنى فان غالبية النصوص تحمي الحق في حرمة المسكن وسرية الاتصالات (المفهوم المادي للخصوصية ) ، ومعظم الدساتير الحديثة تتضمن نصوصاً خاصة تعترف بالحق في الوصول والسيطرة على المعلومات ( البعد المعنوي للخصوصية ) ، وحتى في الدول التي لم تتضمن دساتيرها أو قوانينها اعترافاً بالخصوصية فان المحاكم فيها قد أقرت هذا الحق بشكل أو بآخر أو استناداً إلى الاتفاقيات الدولية التي اعترفت بهذا الحق حيثما تكون الدولة عضواً فيها . كما يلاحظ ان غالبية الدساتير الحديثة<sup>(٤)</sup> قد تضمنت نصوصاً صريحة بشأن حماية

(١) تنص المادة (١٢) من الاعلان العالمي لحقوق الانسان الصادر سنة ١٩٤٨ على " لا يجوز تعريض احد لتدخل تعسفي في حياته الخاصة او في شؤون اسرته او مسكنه او مراسلاته ، ولا لحملات تمس شرفه وسمعته . ولكل شخص حق في ان يحميه القانون من مثل ذلك التدخل او تلك الحملات " .  
(٢) تنص الفقرة (١) من المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية الصادر سنة ١٩٦٦ على " لا يجوز تعريض أي شخص على نحو تعسفي او غير قانوني للتدخل في خصوصياته او شؤون اسرته او بيته او مراسلاته ، ولا لأي حملات غير قانونية تمس شرفه وسمعته " .  
(٣) تنص الفقرة (١) من المادة (٨) من الاتفاقية الأوروبية لحقوق الانسان الصادرة في روما سنة ١٩٥٠ على " لكل انسان حق احترام حياته الخاصة والعائليه ومسكنه ومراسلاته " .  
(٤) من هذه الدساتير : أ. دستور أسبانيا لعام ١٩٧٨ حيث تنص المادة (٤/١٢) على ان "القانون هو الذي يحدد البيانات التي تخضع للمعالجة الالكترونية ، لضمان الكرامة والحصانة الشخصية والأسرية للمواطنين في ممارستهم لحقوقهم" .

الخصوصية ببعديها المادي والمعنوي ، وان عدداً منها تضمن نصوصاً بشأن حماية الحق في البيانات الشخصية والوصول إليها وادارتها<sup>(٢)</sup> .

ان مسألة خصوصية المعلومات قد أثارت اهتمام المنظمات العالمية والإقليمية ، والتي أكدت على حق الانسان في حرمة خصوصية معلوماته من أخطار الاعتداء على البيانات الشخصية ، حيث برز في هذا الإطار جهود منظمة الأمم المتحدة والمجلس الأوروبي ومنظمة التعاون الاقتصادي<sup>(٣)</sup> .

ففي ظل منظمة الأمم المتحدة تم عقد أول مؤتمر دولي في ميدان حماية خصوصية المعلومات في مواجهة أخطار التقدم التقني ( مؤتمر طهران لعام ١٩٦٨ ) وتبنت الجمعية العامة للأمم المتحدة توصياته والتي ابرز ما جاء فيها " ان الحاسبات الإلكترونية تمثل اكبر تهديد للحياة الخاصة والحرية الشخصية ، اذ انها تعد من أدوات المراقبة وأجهزة التطفل الحديثة ، وخاصة إذا تم تخزين البيانات الشخصية على الحاسب الآلي وتحليلها ، مما يكشف عن انماط التعامل والعلاقات<sup>(٤)</sup> .

وعلى الصعيد الإقليمي برز دور مجلس أوروبا والسوق الأوروبية المشتركة ، وذلك بتوقيع معاهدة<sup>(٥)</sup> مجلس أوروبا والخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية ، ويقتصر نطاق تطبيق هذه الاتفاقية التي بدأ السريان الفعلي لها في أكتوبر ١٩٨٥ على الأشخاص الطبيعيين ، وتسري على القطاعين العام والخاص بشأن الملفات المعدة آلياً ، حيث تحظى بالزامية أحكامها لتحقيق حماية البيانات الشخصية المعالجة آلياً .

ب. دستور البرتغال لعام ١٩٧٦ حيث تنص المادة (١/٣٥) على ان : " لكل المواطنين الحق في معرفة المعلومات التي تتعلق بهم وما تتضمنه بنوك المعلومات من بيانات خاصة بهم ، والاستخدامات المعدة لها ، ويكون لهم طلب تصحيحها أو تصويبها أو الإضافة عليها كل فترة عندما يطراً عليها تغيير " .  
ج. دستور النمسا : حيث نص في مادته الأولى على حماية البيانات ذات الصبغة الشخصية .

(٢) W W W . international privacy . org

(٣) المحامي يونس عرب ، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي ، بحث مقدم إلى منتدى العمل الإلكتروني ، اتحاد المصارف العربية ، المنعقدة في عمان في الفترة ما بين ٢٠ - ٢٢ أيار عام ٢٠٠١ ، ص ١٢ .

(٤) يونس عرب ، جرائم الحاسوب ، دراسة مقارنة ، رسالة مقدمة لنيل درجة الماجستير في الحقوق ، كلية الدراسات العليا ، الجامعة الأردنية ، ١٩٩٤ ، ص ١٢٥ .

(٥) وقعت على الاتفاقية كل من ( النمسا ، بلجيكا ، الدنمارك ، ألمانيا ، فرنسا ، اليونان ، إيطاليا ، البرتغال ، السويد ، تركيا - لوكسمبورج ، النرويج ، المملكة المتحدة ) .



وقد صدر عن مجلس أوروبا العديد من التوصيات<sup>(١)</sup> لتؤكد على توسيع نطاق الحماية، لتشمل قطاعات الأنشطة الخاصة كالبيانات الطبية والبحثية والإحصائية، ... الخ.

ومن الجهود المبذولة أيضا على المستوى الإقليمي ، جهد السوق الأوروبية المشتركة  
المشتركة (البرلمان الأوروبي) ، حيث صدر عن البرلمان الأوروبي عدة قرارات منها ، قرار (٨) نيسان ١٩٧٩ الخاص بحماية الفرد في مواجهة التطور التقني للمعلوماتية ، وكذلك القرار الصادر في (٨) أيار ١٩٧٩ والمتعلق بحقوق الفرد في مواجهة التطورات التقنية في مجال البيانات ، وأيضا القرار الصادر في (٩) آذار لعام ١٩٨٢ والخاص بحماية الفرد في مواجهة التطورات التقنية في مجال معالجة البيانات .

وإذا كان موضوع هذا الفصل ينصب على بيان حماية المعلومات الشخصية للأفراد من أخطار بنوك المعلومات ، فإنه من الضروري إظهار مبادئ الحماية في مبحث أول ، ثم إظهار الضمانات في مبحث ثان .

وفي ضوء ما تقدم سنقسم دراستنا في هذا الفصل إلى المبحثين التاليين :-

المبحث الأول : مبادئ حماية المعلومات الشخصية في بنوك المعلومات .

المبحث الثاني : الضمانات المتاحة للفرد في السيطرة على معلوماته الشخصية .

(١) من أبرز تلك التوصيات :-

١. التوصية رقم ٨٠/١٣ لعام ١٩٨٠ بشأن تبادل المعلومات القانونية المتصلة بحماية البيانات .
  ٢. التوصية رقم ٨١/١ لعام ١٩٨٠ بشأن تنظيم البيانات الطبية المعالجة آلياً في بنوك المعلومات .
  ٣. التوصية رقم ٨٣/١٠ لعام ١٩٨٣ والخاصة بحماية البيانات الشخصية المستعملة للبحوث العملية .
- نقلا عن / يونس عرب ، جرائم الحاسوب ، مرجع سابق ، ص ١٢٨ .

## المبحث الأول

### مبادئ حماية المعلومات الشخصية في بنوك المعلومات

#### تمهيد وتقسيم :-

هناك اتفاق عام بالنسبة لضرورة وجود عدة مبادئ لحماية المعلومات الشخصية إزاء التهديدات الناشئة عن استخدام نظم وأساليب جمع المعلومات الشخصية عن طريق بنوك المعلومات، وكذلك لتحقيق نوع من التوازن بين الفوائد التي تنتج عن استخدام هذه النظم والأساليب ، وبين الحفاظ على حقوق الانسان .

ونتيجة لتظافر جهود الفقه والقضاء والقانون المقارن في كل من فرنسا ، امريكا ، المانيا ، فقد تم الاتفاق على وضع مجموعة من المبادئ ، والتي تهدف إلى وضع الفرد في موقع متقدم في مواجهة تلك الاعتداءات، كي يتمكن من السيطرة على معلوماته باعتبار ان الخصوصية التي تدور حولها الحماية هي خصوصية المعلومات ، ومن ثم فان تلك المبادئ تسعى لتمكن الفرد من السيطرة على المعلومات المتعلقة به والمخزنة عنه آليا في بنوك المعلومات ، كما ان من شان هذه المبادئ ان تقلل من مخاطر الاعتداء على المعلومات أو البيانات الخاصة للأفراد إذا ما تم الأخذ بها والعمل على إبرازها ووجودها في التشريعات العادية ، أما في حالة عدم النص على مثل هذه المبادئ ، فان ذلك سيزيد من فرص الاعتداء والمخاطر على حقوق الأفراد في خصوصية معلوماتهم ، الأمر الذي سيترتب عليه نتائج وخيمة من شأنها الأضرار بمصالح الأفراد .

ولذلك عمدت تشريعات الدول المتقدمة علمياً وتكنولوجياً إلى حماية المعطيات والبيانات الشخصية من خلال إقرارها لمجموعة من المبادئ والتي يمكن من خلالها التقليل من الآثار المحتملة التي تصيب الفرد في خصوصية معلوماته .

ومن هذه المبادئ على سبيل المثال لا الحصر ، مبدأ الأخطار العام ، ومبدأ الأمن ، ومبدأ الوصول إلى البيانات والسيطرة عليها ، وحق الفرد في الاحتفاظ بالمعلومات ، ومبدأ استخدام المعلومة في الغاية أو الهدف الذي أخذت من أجلها ، ومبدأ الإشراف

المستقل وغيرها من المبادئ والوسائل التي يمكن من خلالها المحافظة على خصوصية المعلومات المخزنة إلكترونياً وحمايتها من مخاطر الغير وتطفل الآخرين .

وتأسيساً لما تقدم فإننا سنعرض للمبادئ العامة التي تهدف إلى حماية خصوصية الأفراد في مجال المعلومات والبيانات الشخصية التي تخزن إلكترونياً في بنوك المعلومات وتحد أيضاً من المخاطر التي تصيب الفرد في خصوصية معلوماته وذلك في أربعة مطالب مستقلة وعلى النحو الآتي :-

المطلب الأول :- مبدأ الأخطار العام

المطلب الثاني :- مبدأ الشرعية

المطلب الثالث :- مبدأ الأمن

المطلب الرابع :- مبدأ الحماية المهنية

## المطلب الأول

### مبدأ الأخطار العام

ان هذا المبدأ يعني ان كل نظم الحاسبات الإلكترونية وبنوك المعلومات التي تتعامل في المعلومات الشخصية ، ينبغي ان تكون معلومة للجمهور . ومن مقتضى هذا المبدأ ان الشخص لا يستطيع ان يتحقق من الضرر حتى يعلم به ، ويعلم من هو المسؤول عنه ، ولذلك فمن المهم اكتشاف ما الذي تسجله بنوك المعلومات عن الأفراد، أو ما يحتمل ان تسجله عنهم، وهذا هو أساس مبدأ الأخطار العام ، ولا يعتبر ان هذا المبدأ قد حقق أهدافه ما لم يتمكن الأفراد من معرفة ما يسجل عنهم من معلومات شخصية<sup>(١)</sup>.

عندما تقوم الجهة القائمة على بنوك المعلومات ، بجمع معلومات معينة عن الفرد فانه يقع على عاتقها اخطاره عن هذه المعلومات ، التي ربما قد تستخدم في غير ما خصصت له من أغراض ، فالفرد لا بد وان يعترف له بهذا الحق حتى لا يكون ضحية لانتهاك حقه في الخصوصية دون ان يعلم بذلك ، فقد لا يكتشف مطلقاً بانه كان مادة لملف مخزن آلياً ، كما ان من حقه ان يعرف وبشكل مفصل عن ماهية ونوعية المعلومات التي لدى الجهات المختلفة عنه ، اذا ان ادخال اي معلومة خاطئة ونسبتها اليه قد تلحق به الضرر الذي لا يمكن تعويضه في بعض الاحيان ، من هنا وجب على هذه الجهات ان تخطر الشخص بأن هناك معلومات معينة قد سجلت عنه ، وان من حقه الاطلاع عليها وتصويب الخاطيء منها<sup>(٢)</sup> .

ومن الجدير بالذكر ان الفرد اذا اتيح له ان يعلم بوجود معلومات مخزنة عنه آلياً لدى بنوك المعلومات ، واعطي الحق في الاخطار فان المخاطر والاعتداءات التي تصيبه في خصوصية معلوماته سيقبل اثرها وتتلاشى تدريجياً<sup>(٣)</sup> .

(١) د. ميدر سليمان الويس ، اثر التطور التكنولوجي على الحريات الشخصية في النظم السياسية ، مرجع سابق ، ص ١٢٨-١٢٩ .

(٢) المقاطع ، حماية الحياة الخاصة للأفراد وضمائنها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ١١٠ .

(٣) المرجع نفسه ، ص ١١٠ .

وعلى صعيد التشريعات ، "نبدأ بالقول ان قانون الخصوصية وتبادل المعلومات الأمريكي الصادر عام ١٩٨٨ ، يوجب على الأجهزة الفيدرالية ان تخطر الأشخاص المعرفين في انظمتها، عن وجود الملفات الخاصة بهم ونيتها في تبادل هذه المعلومات عنهم" (٤).

أما في التشريع الفرنسي فان المادة (١٦) (١) من قانون الكمبيوتر والحريات لعام ١٩٧٨ تفرض التزامات على كل شخص يقوم بتسجيل معلومات شخصية عن الأفراد ان يخطر اللجنة الوطنية للمعلوماتية والحريات ، ويلاحظ ان القانون يفرض واجب الأخطار قبل القيام بإدخال المعلومات في الكمبيوتر وقبيل إجراء معالجة البيانات ، وليس قبل جمع هذه المعلومات . كما يلاحظ ان القانون لا يستلزم موافقة اللجنة قبل القيام بعملية التسجيل ، وانما مجرد أخطارها ، وعند أخطار اللجنة على هذا النحو تقوم الأخيرة بمتابعة مهمتها في التحقيق من مدى احترام الأحكام المقررة في هذا القانون (٢).

ويشارك القانون الفرنسي تشريعات أوروبية عديدة في اشتراطها ان يتم هذا النوع من الأخطار إلى جهة تتولى مهمة المراقبة والمتابعة لحماية خصوصية الأفراد ، من ذلك القانون الدنماركي ، والقانون السويدي ، والقانون الإيطالي .

أما في بريطانيا فانه بالرغم من وجود تشريع خاص لحماية المعلومات منذ عام ١٩٨٤ يعطى الفرد هذا الحق ( الأخطار ) وغيره من الحقوق ، إلا ان مكتب سجل حماية المعلومات قد تلقى في عام ١٩٨٩ اكثر من ١١٠٠ شكوى من المواطنين

(٤) Donsia Renee Strong "The Computer Matching and Privacy Protection Act of 1988" P.397

نقلاً عن المقاطع ، المرجع نفسه ، ص ١١٠ .  
(١) المادة (١٦) تنص على " انه عندما يتعلق الأمر بمعالجة لخلاف الجهات المحددة بالمادة (١٥) تعين أخطار اللجنة الوطنية للمعلوماتية والحريات قبيل إجراء معالجة البيانات ، ويجب ان ينطوي هذا الأخطار على إقرار بان المعالجة تتفق ومتطلبات القانون ، وعند استلام الجهة الطالبة ما يفيد العلم بوصول الأخطار للجنة ، كان بإمكانها البدء في معالجة البيانات علماً بان هذا لا يعفيها من مسؤوليتها .

- الجهات المحددة بالمادة (١٥) هي : الدولة ، الهيئات العامة أو الهيئات المحلية ، أو الأشخاص المعنوية الخاصة التي تقوم بإدارة خدمة عامة .  
(٢) غنام ، الحماية الإدارية والجنايئة للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر ، مرجع سابق ، ص ٩٢ .

تتعلق بموضوع حقهم في الاطلاع على المعلومات والأخطار عنها في مواجهة المؤسسات الخاضعة للقانون المذكور<sup>(٣)</sup>.

إذا لا منازعة في ان الحق في الإعلام ( الأخطار ) بوجود معلومات عن الشخص، يعتبر من الضمانات الأساسية لسلامة حق الفرد في الخصوصية ، وهو موضع اهتمام كثير من التشريعات المعاصرة<sup>(٤)</sup>.

وتجدر الاشارة هنا ان تجميع المعلومات وتخزينها عن أي فرد يرتبط بقاعدة هامة فحواها انه يلزم إخطار هذا الشخص بما تم تخزينه من معلومات عنه اذا كانت لأول مرة وتعلقت بحياته الشخصية . فضلاً عن ذلك فان ما يتم جمعه من معلومات يجري تحليله ، إضافة إلى ما يحوط من يحق لهم الاطلاع على هذه المعلومات من دقة وتهديد ، مع ملاحظة ان تحليل المعلومات يجب ان لا يقتصر على ما يقدمه مستخدم المعلومات من اعتبارات ، بل يجب ان يدخل في الحسبان بالدرجة الأولى مصالح الأفراد في عدم تزايد او تكاثر المعلومات الشخصية التي يتم تجميعها عنهم<sup>(١)</sup> .

ومن الجدير بالذكر ان الأردن تعتبر من الدول التي التزمت الصمت نحو أخطار بنوك المعلومات على خصوصية الأفراد ، حيث اكتفت التشريعات فيها بالنصوص الخاصة بحماية الأسرار ولم يوجد تشريع خاص لحماية المعلومات يعطي الفرد حق الإخطار ، وهذا يعتبر قصور في التشريع الأردني ، نتمنى ان يتم تداركه من قبل المشرع .

وفي رأينا فإنه لا بد من إنشاء لجنة متخصصة وفق أحكام القانون ولتكن المركز الوطني لتكنولوجيا المعلومات ، على غرار اللجنة الوطنية للمعلومات والحريات في فرنسا، حيث تكون مهمة هذه اللجنة المراقبة والمتابعة لحماية خصوصية الأفراد وحماية معلوماتهم الشخصية ويمكن عن طريقها إعلام الشخص بان هناك معلومات قد تم تسجيلها عنه ، مما يمكن الفرد من ممارسة حقه في الاطلاع على هذه المعلومات وتصويبها .

(٣) المقاطع ، مرجع سابق ، ص ١١١ .

(٤) walter F.Pratt "the Warren and Brandeis Argument For Aright to Privacy " P . 179

نقلًا عن المقاطع ، مرجع سابق ، ص ١١١ .

(١) د. محمد عبد العظيم محمد ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث ، مرجع سابق ، ص ١١٦٤

## المطلب الثاني

### مبدأ الشرعية

يعتبر هذا المبدأ واحداً من أهم المبادئ لحماية البيانات والمعلومات الشخصية للأفراد ، عند تخزينها في بنوك المعلومات ، ويمكن فهم هذا المبدأ من خلال نقطتين رئيسيتين هما :-

أولاً : ينبغي استخدام المعلومات الشخصية المعدة بوساطة بنوك المعلومات في الأغراض المشروعة .

حيث تبين ان الغرض والهدف من هذا المبدأ هو ان المعلومات الشخصية المعدة والمخزنة في بنوك المعلومات ، ينبغي جمعها واستخدامها في الأغراض المشروعة فقط . فعلى سبيل المثال فان بيانات التعداد والإحصاءات السكانية التي تؤخذ عن الأفراد ، يجب ان تستخدم في الغرض الذي جمعت من اجله هذه البيانات ، ولا يجوز استخدامها في أغراض غير مشروعة كان تستخدم للإدانة الجنائية ، أو لترتيب أي عبء مالي ، أو لفرض ضريبة معينة .

وتطبيقاً لذلك قضت المحاكم الألمانية في سبيل الحماية للبيانات التي تتعلق بالحياة الخاصة بوقف إحصاء عن السكان في ١٩٨٤ بعد ان ثبت لها ان وزارة الداخلية استطاعت من خلال استمارات الإحصاء الحصول على عناوين مجموعة متطرفة إرهابية مما يعد إساءة لاستخدام البيانات التي جمعت من اجل غاية معينة ، وهي الإحصاء السكاني ، ويشكل اعتداء على الحياة الخاصة للأفراد ، وانتهاكاً لأسرية البيانات<sup>(١)</sup> .

ونرى أن وزارة الداخلية الألمانية قد انحرفت عن الهدف أو الغاية التي من اجلها تم تجميع المعلومات عن الأفراد ، فهي من خلال التعداد العام للسكان ، استطاعت ان تحصل على عناوين مجموعة إرهابية ، مما يعد إساءة لاستخدام البيانات وانحرافها

(١) ادم عبد البديع ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي، مرجع سابق ، ص ٥٠٥ .



عن الغرض المقصود ، حيث انه لا يجوز استخدام المعلومات والبيانات الإحصائية للإدانة الجنائية وهذا يعد انتهاكاً لخصوصيات الأفراد وافتتات واعتداء على حرياتهم .

ومن المعلوم ان استخدام هذه المعلومات يتم الاتفاق عليه مع صاحب المعلومات أو بموجب نص قانوني يترتب على مخالفته توقيع العقاب ، ويجب أيضاً ان يعرف الشخص الذي تسجل عنه هذه المعلومات الغرض الذي من اجله تستخدم المعلومات التي تخصه ، وان يكون هذا الموضوع واضحاً له .

وفي بريطانيا يرى الفقيه (Younger) انه يجب قصر استخدام المعلومات فيما جمعت من اجله ، بمعنى انه لا يجوز استخدام البيانات والمعلومات في غير الأغراض التي جمعت من اجلها، ما لم يتم الحصول على إذن مسبق من أصحابها ، ويجب وضع الضمانات ضد إفشائها أو نقلها إلى من لا يحق لهم معرفتها<sup>(١)</sup> .

كما يقوم بمناشدة الجمهور باليقظة وبخلق روح جديدة تماماً من الحماية الذاتية للنفس ، ويجب تشجيع الناس على عدم تقديم أية معلومات أو بيانات ما لم يكونوا مقتنعين تماماً بالغرض الذي طلبت من اجلها ، وحتى تكون هناك الضمانات القانونية الملائمة للحفاظ على سريتها .

ثانياً : ينبغي استخدام المعلومات الشخصية بموجب القانون للمصلحة العامة :

ليس ثمة صعوبة إذا كان استخدام المعلومات مذصوص عليها في القانون ، أما الحالات التي تقبل التأويل ، فيجب ان يفصل فيها طرف ثالث وفقاً لمبدأ الإشراف المستقل ، ولكن هناك حالات يرغب فيها مشغل الحاسب الإلكتروني أو القائم على بنوك المعلومات ان يستخدم المعلومات الشخصية في غرض لم يوافق عليه الشخص الذي تخصه هذه المعلومات ، وفي حالة عدم وجود نص عقابي على استخدام المعلومات ، يكون الغرض الجديد للمعلومات مهماً للغاية وهو استخدامها للمصلحة العامة<sup>(٢)</sup> . وفي حالات كثيرة يكون من الأفضل للمسؤول عن نظام المعلومات ان يستطلع رأي صاحب المعلومات ليحصل على موافقته بشأن الغرض الجديد ، وإذا كان المسؤول عن نظام

(١) Paulsieghart : Privacy and Computers . Latimer New dimension limited London 1976 P.111-113

نقلاً عن / محمد عبد العظيم ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث ، مرجع سابق ، ص ١١٨١ .

(٢) المرجع نفسه ، ص ١٨٢

المعلومات قطاعاً عاماً يمكن ان يستطيع إقناع البرلمان بسن قانون جديد يجيز استخداماً آخر للمعلومات<sup>(٣)</sup> .

ومن الواضح إذا توافرت ضرورة قوية للمصلحة العامة لاستخدام المعلومات لأغراض جديدة، فانه من الحكمة ان تكون هناك جهة لها سلطة الترخيص ويفضل ان تكون مستقلة عن كل الأفراد ومشغلي بنوك المعلومات ، تستطيع ان ترخص باستخدام هذه المعلومات ، وتكفل لهذه الجهة كل الضمانات ، وهذا يؤدي بنا مرة أخرى إلى مبدأ الإشراف المستقل<sup>(١)</sup> .

وفي هذا الصدد نسوق حكماً قضائياً - بالرغم من ندرتها في هذا المجال - صادراً عن القضاء في جمهورية المانيا الاتحادية بتاريخ ١٦/٧/١٩٦٩<sup>(٢)</sup> بشأن اختراق المعلومات الشخصية في أجهزة بنوك المعلومات ، وما يترتب على ذلك من انتهاك لخصوصية الأفراد.

وفي هذا الحكم انتهت المحكمة الدستورية لجمهورية ألمانيا الاتحادية إلى أن لجوء الحكومة إلى إلزام الأفراد بتقديم معلومات شخصية وتسجيلها في بنوك المعلومات أمر تأباه الكرامة الإنسانية وترفضه القيم التي تحترم المرء لأدميته ، وخلصت المحكمة إلى أن هذا الأسلوب من جانب الحكومة ينطوي على مساس وتطفل وانتهاك لخصوصيات الأفراد ، ومن ثم فإنه يعد أمراً غير دستوري ، تأسيساً على ما للشخصية الإنسانية من احترام واجب ، وينبغي أن يترك للمرء الحرية في ان يتمتع بحياته الخاصة دون تدخل أو إزعاج من جانب الدولة .

ونؤيد ما ذهب اليه الدكتور محمد عبد العظيم في تعليقه على الحكم ، حيث إن المحكمة لم تذهب إلى إطلاق هذا الحق ولكنها قيدته بما يتواءم مع بعض جوانب المصلحة العامة للمجتمع ، بدليل أنها استطردت تقول : ومع ذلك فانه ليس بالضرورة اعتبار كل تدخل في حياة الفرد بالحصول على معلومات عنه يعتبر تطفلاً واعداء على كرامة الإنسان مما يتعارض مع الدستور . فالفرد عضو في المجتمع وهو بهذه الصفة

(٣) مبدر لويس ، اثر التطور التكنولوجي على الحريات الشخصية للنظم السياسية ، مرجع سابق ص ١٣٠ .

(١) د. مبدر سليمان الويس ، اثر التطور التكنولوجي على الحريات الشخصية في النظم السياسية ، مرجع سابق ، ص ١٣٠ .

(٢) رقم الحكم : E / CN . 4 / 1066 / Add . 101 . PP-3-4  
نقلاً عن / محمد عبد العظيم ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث ، مرجع سابق ، ص ١١٧٠ .

يجب ان يتجاوب إلى حد معين مع ما تجريه الحكومة من دراسات إحصائية في مجال التخطيط العلمي وحتى تتمكن من إصدار أحكام على أسس وبيانات سليمة ، بشرط ان لا تشمل البيانات الإحصائية ما يتعلق مباشرة ب حياة الأفراد الخاصة وإلا نكون بصدد إساءة لاستخدام المعلومات ، أما إذا اقتصرَت البيانات على دراسة السلوك الخارجي فإنها لا تكون بذلك قد تعارضت مع المبدأ العام الواجب احترامه و هو الحفاظ على شخصية الإنسان وكرامته .

## المطلب الثالث

### مبدأ الأمن

ان هذا المبدأ يعني ان المعلومات الشخصية التي تخزن في أجهزة بنوك المعلومات يجب ان تكون في مأمن من وصول غير المرخص لهم إليها ، وان واضعي الضمانات يهدفون إلى إيجاد ضمانات مناسبة تضمن احترام الآخرين لخصوصية البيانات التي تجمع عن الأفراد في أجهزة الحاسبات الإلكترونية . بعبارة أخرى فان واضعي الضمانات يهدفون إلى حماية المعلومات من الاعتداء عليها من قبل الغير ، بصرف النظر عن الدوافع والوسائل الفنية التي يحتمل ان تستخدم. واهم الضمانات التي يطالبون بتحقيقها هي (١) :-

١. ان تكون المعلومات الشخصية المخزنة إلكترونياً سليمة .
٢. لا يجوز لغير من له الحق فعلاً الاطلاع عليها .
٣. التأكد من استخدام المعلومات فيما خصصت له من أغراض .
٤. ضرورة تصحيح الخطأ إذا تأكد وقوعه .

ومن اجل توقي مخاطر المعلوماتية وحفاظاً على المعلومات وأمنها من وصول الغير، قامت الدول الصناعية الحديثة بإصدار التشريعات اللازمة لحماية المعلومات الشخصية في مواجهة بنوك المعلومات ، فأصدرت السويد قانون حماية البيانات في سنة ١٩٧٣ ، وكذلك قامت الولايات المتحدة الأمريكية بإصدار قانون الخصوصية في سنة ١٩٧٤ وقامت أيضا النرويج بإصدار قانون بشأن ضوابط تسجيل البيانات الشخصية في سنة ١٩٧٨ .

ومن خلال التشريعات المقارنة نجد ان جمهورية ألمانيا الاتحادية قد أكدت على هذا المبدأ من خلال قانون ولاية هيسن (Hessen) لحماية البيانات (٢) ، والذي يهدف

(1) نفس المرجع السابق ص ١١٧٨ .

(٢) ومن الملاحظ ان جمهورية ألمانيا الاتحادية هي الدولة الوحيدة التي أوجدت تشريعاً وافياً عن بنوك المعلومات قبل صدور قانون الخصوصية الأمريكي سنة ١٩٧٥ ، ويعتبر هذا القانون أول تشريع من نوعه في العالم يتناول اثر بنوك المعلومات على الفرد والمجتمع .  
للمزيد / انظر د. محمد عبد العظيم محمد ، مرجع سابق ، ص ١١٩٣ وما بعدها .

إلى منع إساءة استخدام المعلومات المجمعة إلكترونياً في بنوك المعلومات ، ويفرض حماية مزدوجة على هذه البنوك، فهو :

أولاً : يقضي بجمع ونقل وتخزين السجلات والبيانات بطريقة لا تسمح لغير المرخص لهم بالحصول على استشارات منها أو تغييرها أو استخلاصها أو إعدامها .

ثانياً : يفرض السرية على الأشخاص المسؤولين عن جمع وتخزين واعداد البيانات ، ويعد مخالفة أي إفشاء للمعلومات سواء كان مقصوداً أو نتيجة إهمال ، ويحق للجهة التي وقع عليها الضرر ان تطلب تصحيح البيانات الخاطئة ، كما ويحق للفرد الذي اعتدى على حقوقه نتيجة للحصول على البيانات أو تغييرها أو إعدامها أو استخلاصها بدون وجه قانوني وقف الاستمرار في مثل هذه الأعمال . كما ان الحماية التي يقدمها هذا القانون للمعلومات تغطي كل السجلات المعدة لأغراض إعداد المعلومات إلكترونياً والتي تحتفظ بها سلطات الولاية والهيئات العامة والمنشآت في الاختصاص الإقليمي للولاية (١).

ثالثاً :- وتطبيقاً لهذا القانون ( قانون هيسن ) تم تعيين قاض مفوض لحماية البيانات ، وهو مسؤول عن تنفيذ مواد القانون ، ويقوم بحل المشاكل المتعلقة بأعمال بنوك المعلومات ، ويستطيع ان يبادر باتخاذ إجراء ما دفاعاً عن أي شخص يرى انه قد اعتدى على حقوقه ، ويقع عليه واجب تبليغ السلطات المسؤولة عن أي خروج على القانون ، وتقرير ما يراه من وسائل بشأن ضمان حماية المعلومات .

رابعاً :- يضمن قانون هيسن ما يلي :-

- ١ . فرض واجب حماية الثقة أو السرية في طريقة تشغيل جميع بنوك المعلومات .
- ٢ . فرض واجب السرية على العاملين مع تقرير العقوبات للمخالفين .
- ٣ . إعطاء الفرد حق تصحيح الأخطاء .
- ٤ . إجراءات خاصة بالشكاوي عن طريق قاضي حماية البيانات .
- ٥ . حق البرلمان في الحصول على المعلومات .

(١) هناك عدد من الدول تدرس احتمالات مثل هذا التشريع ، ومنها كندا ، الدنمارك ، السويد ، النرويج ، المملكة المتحدة.

إن هذا القانون يهدف - وبحق - إلى حماية المعلومات المعدة إلكترونيا من إساءة استخدامها، وفائدته تبدو في حماية المعلومات الشخصية طالما أنها مخزنة في بنوك المعلومات ، أو معدة بالوسائل الإلكترونية ، أو بوساطة مكاتب إدارية عامة ، أو منشآت حكومية ، أو بوساطة أشخاص أو جمعيات أخرى مؤسسة بموجب قانون خاص محدد لأغراضها الخاصة .

ووفقاً لهذا القانون ينبغي أخطار الشخص عند اختزان معلومات شخصية عنه لأول مرة ما لم يعلم باختزان تلك المعلومات بطريقة أخرى

وبمقتضى هذا القانون يعاقب بالحبس لمدة لا تتجاوز سنة أو بالغرامة أي شخص أو أشخاص يتبادلون أو يحصلون على مستخرج من بنك المعلومات دون موافقة صاحب الشأن ، كما يعاقب بالغرامة أو الحبس لمدة لا تتجاوز سنتين أي شخص يعد معلومات على نحو غير لائق أو يحصل على معلومات شخصية سواء بقصد المنفعة أو بقصد الأضرار بشخص آخر<sup>(١)</sup>.

وفي المملكة المتحدة كان من دواعي الخوف على تهديد خصوصية الأفراد بسبب استخدام بنوك المعلومات ، وتأكيدياً لحماية الخصوصية ، ان صدر قرار بشأن بنوك المعلومات عام ١٩٧٠ ، وكان مبعث هذا القرار الخشية من تهديد الحق في الخصوصية بسبب طبيعة عمل تلك البنوك بصفة عامة ، حيث اصدر وزير الداخلية قراراً بتشكيل لجنة برئاسة ( Younger ) لبحث مسألة الخصوصية ، ومن بين ما تمخض عن هذه اللجنة المقترحات التالية<sup>(٢)</sup> :-

١" يجب النظر إلى المعلومات على أنها أخذت لغرض معين ، ويجب عدم استخدامها في غير ما خصصت له بدون ترخيص .

٢. يجب التأكد من دقة المعلومات المخزنة ، وإتاحة تصحيحها حال وجود أخطاء، أو في حالة تجديد المعلومات .

٣. يجب تعيين الأوقات التي يمكن استبعاد بعض المعلومات التي لا حاجة لها .

(١) محمد عبد العظيم محمد ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث ، ص ١١٩٧ .  
(٢) Report of the Committee on Privacy Kenneth Younger , London 1972 , P . 182-

184  
نقلًا عن / الويس ، اثر التطور التكنولوجي على الحريات الشخصية في النظم السياسية ، مرجع سابق ، ص١٦٤-١٦٥ .

٤. يجب عدم التوسع في حجم المعلومات المجمعة ، وقصرها على غرض محدد.

٥. يجب قصر معرفة المعلومات على المرخص لهم وفي الأغراض التي صدرت بخصوصها تلك المعلومات .

٦. يجب تعيين الوسائل التي يمكن بواسطتها كشف أي اعتداء يتهدد نظام الأمن في أجهزة نظم المعلومات .

٧. انشاء هيئة إشراف مركزية مستقلة ، تضم بعض الشخصيات المتخصصة ، ويكون لها حق تقديم بعض التوصيات بخصوص الضوابط التشريعية أو الضمانات المتعلقة بأسلوب معالجة البيانات والحفاظ عليها " .

وفي رأينا فإن هذه المقترحات مجتمعة ليست لها صفة الإلزام ولكن تم الأخذ ببعض هذه المقترحات في النظم القانونية المختلفة ، فعلى سبيل المثال فان معظم قوانين حماية البيانات تأخذ بمبدأ تحديد الغرض أو الغاية من الحصول على البيانات واستخدامها في أغراض مشروعة ، وتأخذ أيضاً بمبدأ الوصول إلى المعلومات والإطلاع عليها وحق تصحيحها ، وهذا ما نلاحظه في قوانين الولايات المتحدة الأمريكية وخاصة القوانين التي تنص على حماية البيانات الشخصية من خطر إساءة استخدامها بواسطة بنوك المعلومات ، والقانون الذي يقرر للأفراد حق الوصول إلى البيانات الصادر سنة ١٩٧٠ ، كما أخذ ببعض هذه المبادئ المشرع الدنماركي حيث اصدر قانون خاص بحماية البيانات الشخصية المعالجة إلكترونياً عن طريق بنوك المعلومات العامة .

## المطلب الرابع

### مبدأ الحماية المهنية

يعتبر هذا المبدأ واحداً من أهم مبادئ حماية المعلومات الشخصية في مجال تجميعها في بنوك المعلومات ، ويعتمد هذا المبدأ على عدة أمور منها :-

أولاً : الاعتماد على مسلك العاملين في مهنة الكمبيوتر :

ان حماية خصوصية الأفراد من التهديدات والأخطار الناشئة عن استخدام البيانات الشخصية المجمعة إلكترونيا يعتمد إلى حد كبير على مسلك العاملين في مهنة الكمبيوتر واتجاهاتهم ومواقفهم، فهؤلاء الأشخاص لهم دور أساسي في الحفاظ على أمن المعلومات وسلامتها ، وفي القضاء على المشكلات الفعلية أو المحتمل حدوثها والأخطار التي تهدد حقوق الانسان، وذلك إذا ما اهتموا بالحقوق الفردية ، وإذا ما طبقوا بحزم الضمانات التكنولوجية والضمانات القانونية<sup>(١)</sup> .

ومن الناحية الأخرى يمكن القول - بحق - بأنه مهما بلغت الضمانات الفنية من الدقة والتعقيد ، ومهما كانت الضمانات القانونية ، فإن كل ذلك يمكن ان ينهار من جانب العاملين داخل الجهاز أنفسهم ، حيث يستطيعون ان يكونوا مصدر تهديد وخطر على الأشخاص الذين جمعت عنهم المعلومات ، لان هذه المعلومات وان حُجبت عن الآخرين خارج الجهاز بفعل الضمانات إلا انها في متناول العاملين داخل الجهاز<sup>(٢)</sup> .

ثانياً : الكفاءة في التدريب والمستويات المهنية الجيدة للعاملين على أجهزة بنوك المعلومات:

ان الضمانات المطلوبة لحماية المعلومات الشخصية تكمن بصفة عامة في التدريب والمستويات المهنية الجيدة للعاملين الذين يشرفون على الكمبيوتر ، وهي الضمانة الأولى ضد إساءة استخدام بنوك المعلومات ، كما ان موظفي أجهزة بنوك

(١) محمد عبد العظيم ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث ، مرجع سابق ، ص ١١٨٢  
(٢) المرجع نفسه ، ص ١١٨٢ وما بعدها .



المعلومات هم اضعف حلقة في سلسلة الأمن ، لانهم هم الذين لديهم المعلومات الفنية ،  
والفرصة كبيرة للتلاعب في هذه البيانات المخزنة بالأجهزة ، باعتبار ان المعلومات في  
متناول أيديهم (٣).

ثالثاً: الاقتراح بوضع موثيق شرف خاصة لمهنة الكمبيوتر :

باعتبار ان أجهزة الكمبيوتر هي أجهزة تخزين المعلومات الخاصة بالأفراد ،  
نتيجة تجميعها وحفظها ، وتبادل هذه المعلومات عن الأفراد لدى الجهات المختلفة ،  
مما يؤدي إلى إساءة استخدامها والحاق الضرر بالأفراد ، فانه تم اقتراح وضع موثيق  
شرف خاصة بمهنة الكمبيوتر على غرار موثيق الشرف الخاصة ببعض المهن كمهنة  
الطب والصحافة والمحاماة، يحترمها العاملون ويلتزمون بها ، ضماناً لسرية  
المعلومات وعدم إفشائها وإساءة استخدامها في المستقبل(١).

وتجدر الإشارة هنا إلى انه لا يوجد تشريعات معينة قد أقرت مثل هذه الضمانة  
ولكن الفضل يعود في مثل هذا الإقتراح إلى الفقه ، وذلك للتقليل من المخاطر التي  
تصيب الفرد في خصوصية معلوماته نتيجة جمع وتخزين المعلومات وتبادلها عن  
الأفراد لدى الجهات التي تتعامل مع هذه البنوك ، مما قد يؤدي إلى إساءة استخدامها  
والحاق الضرر بالأفراد . من هنا تم الاقتراح بوضع موثيق شرف خاصة بهذه المهنة .

اما بالنسبة لموقف المشرع الأردني من هذه المبادئ فاننا نستطيع القول انه من  
خلال قراءة النصوص الخاصة بحماية البيانات الشخصية للأفراد ، وخاصة المادة  
(١١) من قانون الإحصاءات العامة ، فقد تبين ما يلي :-

١. اخذ بمبدأ المشروعية ويفهم ذلك من خلال نص الفقرة (أ) من تلك  
المادة المتعلقة بالإحصاء والتعداد السكاني ، حيث انه لا يجوز استخدام  
المعلومات المجمعة عن الأفراد لأي غرض غير إعداد الجداول  
الإحصائية ، وبالتالي فإن أي انحراف عن الغرض الأصلي من جمعها

(٣) الويس ، اثر التطور التكنولوجي على الحريات الشخصية في النظم السياسية ، مرجع سابق ، ص  
١٦٤ .

(١) هذه الموثيق تبنى على بعض القواعد السلوكية والمعايير الخلقية مثل الشعور بالمسؤولية وتنمية الإحساس  
بها ومثل النزاهة والأمانة وسلامة النية والثقة والسرية في العمل وعدم الإساءة إلى الآخرين . وقد ظهرت  
عدة محاولات في أمريكا وبريطانيا لوضع لائحة للعاملين في برامج الكمبيوتر ، ولكنها لم تبعد كثيراً عن  
مرحلة الاستدلال .

نقلاً عن / محمد عبد العظيم ، مرجع سابق ، ١١٨٣ .

يعد انتهاكاً واعتداءً على هذه المعلومات التي من شأنها أن تتهدد المصالح المختلفة للأفراد.

٢. اخذ أيضاً بمبدأ الأمن ، حيث يفهم ذلك من خلال الفقرة (د) من المادة السابقة والتي ألزم فيها المشرع الدائرة أن تتخذ كافة الاحتياطات والإجراءات اللازمة من أجل المحافظة على أمن المعلومات التي يتم جمعها عن الأفراد ، وحتى تكون هذه المعلومات في مأمن من وصول غير المرخص لهم بالاطلاع عليها، وان تتوافر في تلك الأماكن شروط الأمان والسلامة وذلك تجنباً لتسرب هذه المعلومات إلى الغير .

٣. كما اخذ المشرع بمبدأ الحماية المهنية وذلك من خلال مسلك العاملين أو الموظفين في الدائرة ، حيث يفهم ذلك من خلال الفقرة (ج) من المادة السابقة والتي يلزم بها المشرع الموظف الذي يعمل في الدائرة بعد أداء القسم التوقيع، على تعهد يلتزم بموجبه بعدم إفشاء أو نشر أي بيانات أو معلومات تتعلق بالأفراد التي تم اخذ المعلومات عنهم .

والخلاصة : ان تلك المبادئ تهدف إلى تقرير حماية خصوصية المعلومات الشخصية التي تجمع إلكترونياً ، ومجمل تلك المبادئ يعني في المقام الأول ان ما يخزن عن الأفراد من معلومات يجب ان يبقى في مأمن من أيدي العابثين والمتطفلين ، كما يعني ضمان استخدامها فيما خصصت له من أغراض ، فالفرد يجب ان يعلم بان هناك معلومات معينة أخذت عنه ، وان من حقه الاطلاع على تلك المعلومات والوصول إليها والسيطرة عليها وتصحيح وتصويب بعض المعلومات الخاطئة . وان من حقه أيضاً محو وتدمير هذه المعلومات عند انتهاء الغرض الذي من أجله أخذت المعلومات .

وفي رأينا ان تلك المبادئ ما لم تدعم بتأييد تام من جانب السلطات العامة في الدولة ، وتصاغ في شكل قواعد دستورية أو قانونية ملزمة فانها لن تتعدى مرحلة التوصيات وبالتالي لن تؤتي ثمارها .

## المبحث الثاني

### الضمانات المتاحة للفرد في السيطرة على معلوماته الشخصية

#### تمهيد وتقسيم:-

حينما تسعى السلطات المختلفة في الدولة إلى الحصول على معلومات من الفرد لغرض من الأغراض كتحديد الضريبة على الدخل أو للاضمان الاجتماعي أو للترخيص الحكومي أو للالتحاق بعمل أو وظيفة ، ثم تستخدم هذه المعلومات للتأثير على الفرد أو اتهامه ، بمعنى إقامة الدعوى عليه في مسائل لا تتصل بالغرض الأصلي الذي من أجله جمعت المعلومات ، فإن هذا يثير سؤالاً حول الإخلال بالثقة التي في ظلها أعطيت هذه المعلومات أصلاً . وكلما تزايد انشاء مراكز رئيسية لتجميع المعلومات عن الأفراد تزايد خطر تسرب هذه المعلومات وانتشارها بشكل غير منضبط ، وهذا يدعو إلى اتخاذ بعض الإجراءات لتصنيف المعلومات إلى فئات مختلفة والتمييز بين حقوق استخدام هذه المعلومات على أساس تلك التصنيفات .

وعلى الرغم من ان هذه الضمانات في مختلف الدول لم توضع في قوانين خاصة لحماية حقوق الأفراد ، ولا سيما في مواجهة الأخطار الفعلية أو المحتملة الناشئة عن استخدام أساليب جمع المعلومات بالوسائل الإلكترونية ، إلا ان القوانين القائمة يمكن ان تضمن هذه الحقوق بشكل عام .

وفي بعض الدول<sup>(1)</sup> صدرت تشريعات يمكن ان تطبق بشكل صريح أو ضمني على أساليب جمع البيانات الشخصية بالوسائل الإلكترونية كمجال البريد والإحصاءات السكانية والائتمان، ... الخ .

وفي عدة دول أخرى<sup>(2)</sup> صدرت تشريعات تتعلق بصفة عامة بأساليب جمع البيانات الشخصية بالوسائل الإلكترونية ، أو جرى اقتراحها أو اقترحت بعض المبادئ في هذا الشأن .

ان البحث في الضمانات أو الوسائل التي تعطى أو تتاح للفرد كي يتمكن من تقليل تلك المخاطر عليه أو السيطرة عليها ، هي الغاية الأساسية المراد تحقيقها ، إذ ان هذه

(1) من هذه الدول ، ألمانيا ، النمسا ، فرنسا ، اسبانيا ، النرويج ، السويد ، بلجيكا .  
(2) مثل : أمريكا ، بريطانيا ، الدنمارك ، كندا ، سويسرا .

الضمانات هي التي تضع الفرد في موقع فعال وعملي في سيطرته على جميع المعلومات المتعلقة به والمخزنة في الحاسبات الإلكترونية كبنوك للمعلومات أو الخاضعة لعملياته المختلفة<sup>(٣)</sup> .

وتجدر الإشارة في هذا المقام إلى ان جميع ما سنعرض له من وسائل أو ضمانات إنما هي إجراءات وقائية أساسا ، وليست إجراءات حماية لاحقة لانتهاكات واقعة على حقوق الفرد، وهذه الإجراءات الوقائية لا تمنع البتة من ان تكون مرتبطة ببعض وسائل الحماية لتحقيق إصلاح الضرر اللاحق ، التي يستلزمها تمكين الفرد من استعمال هذه الضمانات استعمالاً فعالاً ومناسباً موضوعياً وزمنياً في مواجهة تلك الأخطار .

وفي التشريعات المقارنة ، نجد ان الدول المتقدمة علمياً وتكنولوجياً ، قد نصت في تشريعاتها على مجموعة من الضمانات لحماية المعلومات الشخصية من أخطار بنوك المعلومات، والتي يمكن من خلالها ان تتاح للفرد فرصة السيطرة على معلوماته الشخصية ضد إساءة استخدامها من قبل الآخرين أو المتطفلين .

ففي أمريكا مثلاً اصدر الكونجرس عام ١٩٧٤ قانون الخصوصية لحماية المعلومات الشخصية المجمععة إلكترونياً وذلك بهدف حماية هذه المعلومات وصيانتها من عبث السجلات الفيدرالية ، كما نص هذا القانون على مجموعة من الضمانات التي تعطى للفرد من اجل السيطرة على معلوماته الشخصية ، وان تكون هذه المعلومات في مأمن من وصول غير المرخص لهم ، وان من حق الفرد الوصول إلى هذه المعلومات ، وحقه في الاطلاع عليها وتصحيحها وتصويب ما هو خاطئ منها .

ومما لا شك فيه ان الضمانات مهما تعددت انواعها وأشكالها ، سواء كانت ضمانات تشريعية (قانونية) أو ضمانات قضائية أو ضمانات إدارية أو فنية ، فأنها تهدف في نهاية المطاف إلى حماية المعلومات الشخصية الخاصة بالأفراد من سوء الاستخدام وتعطي الفرد الحق في السيطرة على معلوماته الشخصية التي سجلت عنه لدى بنوك المعلومات .

وفي ضوء ما تقدم فإننا سنعرض لمجموعة من الحقوق أو الضمانات المتاحة للفرد في السيطرة على معلوماته الشخصية والتي تخزن إلكترونياً في بنوك المعلومات

(٣) د. المقاطع ، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ٩٥ .

، وتحد أيضا من المخاطر التي تصيب الفرد في خصوصية معلوماته ، وذلك في أربعة مطالب مستقلة وعلى النحو الآتي :-

المطلب الأول :- الحق في الاطلاع على المعلومات التي سجلت عنه

المطلب الثاني :- الحق في تصحيح المعلومات

المطلب الثالث :- الحق في المحافظة على خصوصية المعلومات وسريتها

المطلب الرابع :- الحق في تأقيت المعلومات واستردادها ومحوها والغائها .

## المطلب الأول

### الحق في الاطلاع على المعلومات

من المبادئ الأساسية اللازمة لحماية الحقوق الشخصية في مواجهة بنوك المعلومات، إعطاء الشخص حق الاطلاع على المعلومات الشخصية المتعلقة به والمسجلة في الحاسبات الإلكترونية كبنوك للمعلومات .

ان حق الفرد في الوصول والاطلاع على المعلومات المخزنة آليا عنه يعتبر من اكثر الضمانات فاعلية لحفظ حقه في الخصوصية ، ومن أكثرها تمكيناً له من ممارسة حقه في السيطرة على المعلومات كما تحدث عن هذا الحق الأستاذ ( Vittorio Frosini ) ، عندما قرر بان "الحرية اليوم تكمن في القدرة على التحكم بالمعلومات الشخصية المخزنة في برامج الكمبيوتر" (١) .

فحصول الجهة القائمة على بنوك المعلومات على المعلومات بطريقة مشروعة ، وحفظها وتخزينها طبقاً للقانون أو بعد الحصول على موافقة الشخص في الحالات التي يستلزمها القانون، لا يحول دون ممارسة الشخص للحق في الاطلاع .

وتحرص كافة التشريعات المقارنة ، وخصوصاً القانون الألماني الاتحادي الصادر عام ١٩٧٧ ، والقانون الفرنسي بشأن المعلوماتية والحريات لسنة ١٩٧٨ ، وكذلك الاتفاقية الصادرة من المجلس الأوروبي سنة ١٩٨١ بشأن حماية الحقوق الشخصية في مواجهة المعالجة الآلية للمعلومات ، على إعطاء كل شخص طبيعي حق الاطلاع على المعلومات الشخصية الخاصة به والتي سبق تخزينها لدى أجهزة بنوك المعلومات .

وسنتناول بالدراسة المقصود من الحق في الاطلاع ، ثم سنوضح نطاق هذا الحق واخيراً سنعرض لكيفية ممارسة الحق في الاطلاع ، وذلك في ثلاثة فروع ، وعلى النحو الآتي :-

الفرع الأول : المقصود من الحق في الاطلاع.

(1) Walden & Savage "Data Protection and Privacy Law : Should Organizations be Protected ? In International and Comparative Law Quarterly , Vol P . 337

نقلا عن / المقاطع ، مرجع سابق ، ص ١١١

الفرع الثاني : نطاق الحق في الاطلاع . الفرع الثالث : ممارسة الحق في الاطلاع .

## الفرع الأول

### المقصود من الحق في الاطلاع

يعتبر الحق في الاطلاع مقدمة أساسية وضرورية لممارسة الشخص لحقه في تصحيح المعلومات الشخصية الخاصة به ، وعلى ذلك يقصد بالحق في الاطلاع حق الشخص في ان يعرف كل مضمون المعلومات المسجلة عنه في بنوك المعلومات وطرق معالجتها من اجل ان يمارس حقه في التصحيح إذا كان هناك مقتضى لذلك<sup>(١)</sup> .

والغرض من تقرير حق الاطلاع هو إقامة نوع من التوازن في العلاقة بين الفرد والجهات التي يتعامل معها ، إذا ان حق الفرد في الاطلاع لم يعد حقاً للفرد في مواجهة الدولة فقط ، بل وفي مواجهة القطاع الخاص أيضا ، ولدى أي جهة تتعامل مع بنوك المعلومات .

ويبدو عدم التوازن واضحا في كافة مراحل إقامة نظام المعلومات ، فالفرد يقدم المعلومات بهدف الحصول على ميزة أو بناءً على إلتزام قانوني ، بل في بعض الأحوال قد يتم الحصول على المعلومات دون علمه . كما ان الجهة القائمة على هذه البنوك هي التي تقرر قواعد الأمن الملازمة لتلك المعلومات ، ولها ان تقوم بنقل المعلومات إلى الغير<sup>(٢)</sup> .

وعدم التوازن هذا هو الدافع الأساسي لضرورة وضع نظام قانوني يقيم توازناً في العلاقة سواء بفرض قيود على الجهات القائمة على الحاسب الآلي أو تقرير حقوق لمن تتعلق بهم المعلومات الشخصية المختزنة . وتبدو أهمية ذلك في مجال العلاقات الاقتصادية حيث تكون قدرة المشرع الاقتصادي في اتخاذ القرار مرتبطة بتقدير وضعه الائتماني وسمعته التجارية وتحديد قيمة عنصر العملاء ، والمعلومات المتعلقة بهذه الأمور تسجل في بنوك المعلومات للمصارف وغيرها من الجهات التي يتعامل معها ، ولذلك فان حماية الحرية الاقتصادية للمشروع ترتبط بإعطائه حق معرفة ما هو مسجل

(١) المرجع نفسه ، ص ١١١ .

(٢) الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الالكتروني ، مرجع سابق، ص ٤٥ .

عنه لدى هذه الجهات ، ويعتبر الاطلاع الركيزة الأساسية في تحقيق التوازن والعدالة في العلاقات الاقتصادية<sup>(٣)</sup> .

ولقد أثرت مشكلة التخوف من انه إذا ما طلب الشخص الاطلاع على المعلومات الخاصة به ان تقوم الجهة القائمة على بنوك المعلومات بإخفاء أو تغيير بعض المعلومات ، وتفادياً لهذه المشكلة يجوز لصاحب الشأن ان يطلب من القضاء اتخاذ الإجراءات الوقائية اللازمة لمنع تغيير أو إخفاء المعلومات المخزنة لدى هذه الأجهزة .

وتتمثل الخطوة الأولى لممارسة حق الاطلاع في أن يعلم الشخص بتسجيل معلومات شخصية متعلقة به لدى هذه الأجهزة ولحساب جهة معينة ، حيث يعتبر العلم مؤكداً في بعض الحالات عندما يدلي الشخص بنفسه بالمعلومات من اجل إدخالها إلى الحاسب الآلي كبنك للمعلومات ، مثل المعلومات المقدمة لمصلحة الأحوال المدنية أو للضمان الاجتماعي أو لشركات التأمين .

بيد انه إذا لم يكن الشخص على علم مسبق بوجود معلومات عنه ، فان حق الاطلاع يستوجب إعطاء الشخص الحق في ان يستعلم من الجهة القائمة على بنوك المعلومات عما إذا كانت هناك معلومات شخصية تتعلق به ، وعلى أية حال فان الاستعلام يعد حقاً مستقلاً في حد ذاته ، ويعتبر مقدمة لممارسة حق الاطلاع وحق التصحيح إذا كانت المعلومات الشخصية قد أدخلت إلى أجهزة بنوك المعلومات<sup>(١)</sup> .

ومن الجدير بالذكر ان بعض التشريعات<sup>(٢)</sup> المقارنة تلزم الجهة التي تحصل على معلومات شخصية بغرض تخزينها ومعالجتها لدى أجهزة بنوك المعلومات ان تخطر الأشخاص عند تقديمهم للبيانات بوجود حق الاطلاع والتصحيح فيما يتعلق بتلك المعلومات .

وإذا كان للشخص الحق في الاستعلام من جهة ما عما إذا كان لديهم معلومات عنه ، فان التساؤل يثور عما إذا كان يتعين على الجهة القائمة على هذه البنوك ان تخطر من تلقاء نفسها الأشخاص بوجود معلومات شخصية عنهم من اجل السماح لهم بممارسة الحق في الاطلاع والتصحيح .

(٣) حسبو ، حماية الحريات في مواجهة نظم المعلومات ، مرجع سابق ، ص ١٣٣ - ١٣٤ .

(١) الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني ، مرجع سابق ، ص ٤٦  
(٢) من هذه التشريعات ، التشريع الفرنسي ، الألماني ، الأمريكي ، ... / المرجع نفسه ، ص ٤٦ .



ومن هنا فإن الجهة القائمة على نظام المعلومات الآلية تلتزم بان تخطر الشخص بان لديها معلومات تتعلق به ، لكي يطلبوا الاطلاع واتخاذ ما يروونه لازماً في هذا الشأن . فلا يجب ان يترك العلم بوجود معلومات لمحض الصدفة التي تدفع الشخص للاستعلام عن وجود معلومات عنه ، بالإضافة إلى ان ترك الأمر لحرية الشخص في الاستعلام يكلف الشخص الحريص عناء ومشقة التوجه بالاستعلام إلى العديد من بنوك المعلومات التي قد يتلقى من بعضها إجابات سلبية<sup>(٣)</sup> .

وعلى الرغم من ذلك فان الاتجاه الغالب<sup>(١)</sup> ، يذهب إلى عدم إلزام بنوك المعلومات بأخطار الأشخاص بوجود معلومات عنهم ، ويرجع السبب في ذلك إلى ان الكثير من الناس لا يهتم بمعرفة ما يوجد عنهم من معلومات شخصية لدى بنوك المعلومات من ناحية . كما ان أخطار كافة الأشخاص بوجود معلومات عنهم يحمل بنوك المعلومات عبء ثقيل إدارياً ومالياً، الأمر الذي يعوق المعلوماتية من ناحية أخرى .

وفي رأينا فان الهيئات الحكومية والمؤسسات والشركات الخاصة تجمع عن الفرد معلومات معينة وتقوم بتخزين هذه المعلومات وحفظها في بنوك المعلومات ، وهنا يجب التفرقة بين نوعين من المعلومات ، معلومات عامة عن الأشخاص ، ومعلومات تتعلق بالأمن، كما يجب الموازنة بين مصلحتين ، مصلحة الدولة في جمع هذه المعلومات ، ومصلحة الفرد في عدم الاعتداء على هذه المعلومات ، التي من شأنها ان تؤثر على سمعة الأفراد وتضر بمصالحهم المختلفة . وهنا نخالف ما ذهب إليه الفقه المقارن في عدم إلزام بنوك المعلومات بأخطار الأشخاص بوجود معلومات عنهم ، بل يجب على هذه البنوك أخطار الأشخاص الذين تم اخذ معلومات عنهم ، حيث ان للفرد الحق في ان يعرف اسم الجهة أو المؤسسة أو الشركة التي طلبت أي معلومات عنه ، وذلك كجزء أساسي من حقه في الاطلاع ، حيث يعتبر هذا الحق أحد الضمانات الأساسية لحق الفرد في الخصوصية ، كما ان من حق الفرد الوصول إلى هذه المعلومات والاطلاع عليها وتصويب ما هو خاطئ منها ، لان نسبة معلومات خاطئة لاحد الأشخاص قد تضر بمصالحه المختلفة كما أشرنا سابقاً .

(٣) المرجع نفسه ، ص ٤٧ .

(١) الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الالكتروني ، مرجع سابق ، ص ٤٨ .

## الفرع الثاني

### نطاق الحق في الاطلاع

يسري حق الاطلاع على المعلومات الاسمية التي يكون الشخص محللاً لها ، ويتضمن الاطلاع على المعلومات الشخصية وطرق معالجتها أديا والأسس التي قام عليها برنامج المعالجة والذي تم فيه استخدام المعلومات الشخصية .

ويذهب الفقه الفرنسي<sup>(١)</sup> إلى ان الحق في الاطلاع لا يتضمن معرفة مصدر المعلومات المخزنة في بنوك المعلومات . وعلى العكس من ذلك فان التشريعات في الولايات المتحدة الأمريكية تلزم الجهات القائمة على هذه البنوك في مجالات الوظائف ، والتسهيلات الائتمانية، ووثائق التأمين ، ببيان مصدر المعلومات ، والقصد من ذلك الإلزام هو تيسير إعداد الشخص لدفاعه تمهيداً لممارسة حق التصحيح .

ومن الملاحظ انه من حيث المبدأ لا يمتد الاطلاع والعلم إلى استخدام المعلومات والجهة التي تستفيد منها ، غير انه يتحقق العلم بذلك من إزام المشرع للجهة القائمة على بنوك المعلومات بان تعلن الغرض من نظام المعلومات والجهات التي توجه إليها المعلومات<sup>(٢)</sup> .

وتبدو أهمية الحق في الاطلاع من خلال اهتمام بعض الهيئات والمنظمات الدولية بهذا الحق كضمانة أساسية للفرد في الوصول والسيطرة على المعلومات الشخصية التي أخذت عنه والمخزنة إلكترونياً لدى بنوك المعلومات . ونشير في دراستنا هذه إلى موقف منظمة اليونسكو في نقطة أولى . ثم إلى موقف هيئة الأمم المتحدة في نقطة ثانية .

أولاً : موقف منظمة اليونسكو :

(١) من هؤلاء الفقهاء : فرايسنيه ، كايزر ، انظر / د. حسام الدين الاهواني ، المرجع نفسه ، ص ٤٩ .  
(٢) المرجع نفسه ، ص ٤٩ .

في عام ١٩٧٠ انعقد اجتماع اليونسكو في باريس لدراسة الحق في الخصوصية بشكل عام والحق في المحافظة على المعلومات الشخصية للأفراد من أخطار بنوك المعلومات بشكل خاص. وتركز النقاش بشكل ملحوظ حول مخاطر بنوك المعلومات على المعلومات الشخصية للأفراد، وان هذه الأجهزة تتمتع بإمكانات خارقة في إعطاء البيانات والملفات ، ولها قدرة فائقة في اختزان المعلومات وسرعة استعادتها واستخدامها ، وتضم قدراً كبيراً من المعلومات تجمعت لديها من عدة مصادر مختلفة ويتم اختزانها في مكان واحد، وان تكنولوجيا هذه الأجهزة يمكن ان تستخدم في المستقبل لتزويد الجهات الحكومية أو قطاع الأعمال بما تحتاجه من معلومات عن الأفراد ، وبشكل يفوق ما هو متاح في الوقت الحاضر .

ولما كان الأمر كذلك فانه بات لزاماً ان يوضع من الضمانات ووسائل الرقابة على اختزان المعلومات ما يضمن عدم سوء استخدامها . ومن تلك الوسائل مثلاً ان نحدد المعلومات الجائز اختزانها ومن له حق تداولها وأغراض هذا التداول ، كما تركز البحث حول حق الأفراد في الاطلاع على ما يجمع ويخزن عنهم من معلومات ومناقشتها ، وتحديد الوسائل التي تمكن من يرى وجهاً للاعتراض بالطعن فيها<sup>(١)</sup> .

#### ثانياً : موقف هيئة الأمم المتحدة :

تم بحث أمر استخدام أجهزة جمع المعلومات الشخصية على مستوى الأمم المتحدة ومدى اثر ذلك على خصوصيات الأفراد.

فعلى الرغم من ان هناك اعترافاً واسعاً بالمزايا العملية لاستخدام أجهزة بنوك المعلومات في رسم السياسات وصنع القرارات والأعمال الإدارية ، إلا أن هناك بعض المخاوف والشكوك التي تساور الكثيرين بالنسبة لتأثير هذه الأجهزة على حقوق الإنسان ، ومن بينها حق الفرد في خصوصية معلوماته .

وقد جاء في تقرير الامين العام للأمم المتحدة أن أجهزة جمع المعلومات تعتبر من أدوات المراقبة ، وأنها تعتبر أفدح تهديد لخصوصية الفرد في الوقت الحاضر . ذلك أن

(١) Unesco Final Report : SHC / CoNF / 11/12 Paris. 19-23 January . 1970 . P.2.3  
نقلاً عن / محمد عبد العظيم ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث ، مرجع سابق ، ص ١١٧٣ .

من أسهل الأجهزة الحديثة للتطفل قلم تسجيل ، بحيث إذا وضع على خط تليفون فانه يسجل أرقام التليفونات التي تم الاتصال بها من تليفون معين ، وهذه القدرة على التطفل يمكنها تجميع اكبر قدر ممكن من المعلومات ، وتقوم بتخزينها لدى هذه البنوك ، بحيث تقوم هذه الأخرى بتحليل هذه المعلومات<sup>(٢)</sup> .

ومن الملاحظ أن هيئة الأمم المتحدة قد أقرت بحق الوصول إلى هذه المعلومات المخزنة لدى الحاسبات الإلكترونية كبنوك للمعلومات والاطلاع عليها وتصويب ما هو خاطئ منها ، وذلك كضمانة أساسية لحق الفرد في السيطرة على معلوماته الشخصية من عبث المتطفلين<sup>(١)</sup> .

### الفرع الثالث

#### ممارسة الحق في الاطلاع

إذا علم الشخص بوجود معلومات شخصية متعلقة به وتم تخزينها لدى أجهزة بنوك المعلومات ، فان من حقه ان يعلم بمضمون هذه المعلومات ، إذ يجب ان تصل تلك المعلومات لعلمه .

ويلاحظ ان هناك ارتباطاً وثيقاً بين الاطلاع والحصول على بيان بالمعلومات الشخصية، ففي كثير من الأحيان يتحقق الاطلاع عن طريق الحصول على البيان . غير ان الحق في الاطلاع لا يعني دائماً وأبداً انه يجوز للشخص الدخول إلى مكان بنوك المعلومات واتخاذ الإجراءات اللازمة للاطلاع على البيانات المتعلقة به مباشرة ، وانما يختلف ذلك وفقاً للظروف والحالات ، حيث قد يكفي الشخص بالحصول على مستخرج من البيانات المسجلة لدى هذه البنوك ، وإذا ساوره شك في ان الجهة القائمة على هذه البنوك لا تستخرج كافة البيانات بل تخفي بعضها فله ان يلجأ إلى المحاكم القضائية

(٢) انظر 23. 4/11169. United Nations Economic and Social Council e/cn. 4/11169. January 1973 Report of the Secretary General P.39-40 .

نقلاً عن / قايد ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، مرجع سابق ، ص ٨١-٨٢ .  
(١) الويس ، اثر التطور التكنولوجي على الحريات الشخصي في النظم السياسية ، مرجع سابق ، ١٤٢

المختصة لتعيين من يقوم بالاطلاع أو تمكينه من الاطلاع مباشرة على المعلومات الخاصة به .

وعلى الرغم من ان الاطلاع يعتبر حق مقرر للشخص ، وضمانة أساسية في المحافظة على صحة المعلومات إلا ان الجهة القائمة على هذه البنوك لا تلتزم بإخطار الشخص بصفة دورية بما يوجد لديها من معلومات ، ويرجع السبب في ذلك إلى انه في كثير من الأحيان لا يهتم الشخص بمعرفة ما يوجد عنه من معلومات لدى هذه البنوك لجهة ما . كما ان إرسال مستخرجات من البيانات المسجلة بصفة دورية قد يهدد بالمساس بخصوصية الفرد إذا وقع المستخرج في يد شخص غير المرسل إليه لأي سبب مثل خطأ البريد أو عدم وضوح العنوان، وأخيراً فإن إلزام الجهات القائمة على هذه الأجهزة بإرسال مستخرجات بصفة دورية يحملها بأعباء مالية وإدارية كبيرة تتعارض مع تطور وتقدم نظم المعلومات<sup>(٢)</sup> .

وفي رأينا ومهما يكن من أمر فإن هذا لا يعفي الجهات القائمة على بنوك المعلومات من مسؤولياتها تجاه إعلام أو إخطار الأشخاص بان هناك معلومات مسجلة عنهم لدى هذه الأجهزة وان من حق هذا الفرد الاطلاع على هذه المعلومات وتصويبها، حيث انه ليس هناك ما يمنع ان تقوم الجهات القائمة على هذه البنوك من إرسال المعلومات دورياً لصاحب الشأن وذلك من تلقاء نفسها ودون إلزام قانوني ، لذا فإن مصلحة الفرد تقتضي إعلامه ضمناً له من سوء الاستخدام لهذه المعلومات ورسم صورة خاطئة عن الفرد تجاه الآخرين ، مما يؤثر بالنتيجة على مصالحه المختلفة .

والاطلاع يكون للشخص نفسه في الأحوال التي يجوز فيها الاطلاع المباشر ، أما في حالات الاطلاع غير المباشر فإن الشخص المخول بالاطلاع هو الذي يكون له فقط حق الاطلاع، أما صاحب الشأن فلا يجوز له ذلك . ومن ثم فإن الاطلاع قد يتم بشكل مباشر أو بشكل غير مباشر ، و سنتناولها بالدراسة فيما يلي :-

#### أولاً : الاطلاع المباشر :

(٢) حسبو ، حماية الحريات في مواجهة المعلومات ، مرجع سابق ، ص ١٤٠ .

يقصد به ان يقوم الشخص المتعلقة به البيانات بالاطلاع عليها بنفسه ، كما يمكن له الحصول على مستخرج .

والحق في الاطلاع لا يجوز النزول عنه مقدماً ويبطل كل اتفاق مخالف ، فضلاً عن ذلك فان هذا الحق حق فردي للشخص وحده ، ولذلك يتعين التحقق بدقة من شخصيته عند طلب الاطلاع ولا يجوز أن يمارس حق الاطلاع عن طريق وكيل ، لان الاطلاع حق فردي لا يمارس عن طريق الغير بحسب الأصل ، أما بالنسبة لناقصي وعديمي الأهلية فان النائب القانوني هو الذي يمارس حق الاطلاع ، ويجوز لصاحب الشأن الاستعانة بمستشار يصحبه معه عند الاطلاع<sup>(١)</sup> .

ولا يلزم صاحب الشأن بتقديم مبررات لممارسة الحق في الاطلاع ، إذا ان هذا الحق مكفول له دون إبداء الأسباب .

ويلزم تقديم المعلومات خلال مدة معقولة ، ولا يجوز تأجيل الرد على طلب الاطلاع إلا إذا كانت الجهة القائمة على هذه البنوك تخطر أصحاب الشأن بصفة دورية بالمعلومات الخاصة بهم حيث يجوز تأجيل الطلب إلى حين حلول موعد إرسال المعلومات الدورية ، ويجب ان يكون الرد كاملاً وواضحاً لا لبس فيه أو غموض ، كما يتعين أن يكون كتابياً وفي لغة واضحة ، ومطابقة تماماً كما هو مختزن في بنوك المعلومات<sup>(٢)</sup> .

ومن الملاحظ في هذا الشأن أن قانون تقارير الأحوال الائتمانية العادلة الأمريكي قد أجاز للفرد الحق في أن يطلع على ما لدى شركات الائتمان المالية من معلومات عنه ، وفي أحوال محددة فقط ، منها حالة حدوث رفض طلب معين له ، أو عدم قبول فتح اعتماد له أو التأمين عليه، استناداً إلى ما لديها من معلومات عنه ، وإلا فانه يلجأ للقضاء لإرغام الشركة على هذا الأمر<sup>(١)</sup> .

## ثانياً الاطلاع غير المباشر :

(١) نفس المرجع السابق ، ص ١٤٢-١٤٣

(٢) الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني ، مرجع سابق ، ص ٥١ .

(٣) John H. f. Shattuck "Right of Privacy" 1966 .p.185

نقلاً عن / المقاطع ، مرجع سابق ، ص ١١٢ .

القاعدة العامة ان الاطلاع يكون من قبل الشخص ذاته وهو ما يسمى بالاطلاع المباشر أما الاطلاع غير المباشر فيعني ان يحظر اطلاع الشخص المتعلقة به المعلومات شخصياً ، وانما يكون الاطلاع لغيره طبقاً لما يحدده القانون . وعلى ذلك فان الأصل هو الاطلاع المباشر ، أما الاطلاع غير المباشر فهو لا يتقرر إلا على سبيل الاستثناء وبناء على نص تشريعي .

واهم صور أو حالات الاطلاع غير المباشر في التشريع المقارن هي :-

١ . الاطلاع على المعلومات المتعلقة بالأمن القومي والأمن العام :

من المسائل الشائكة التي أثارها حق الاطلاع أو الاتصال بالمعلومات الشخصية المختزنة في بنوك المعلومات ، الاطلاع على المعلومات المتعلقة بأمن الدولة والدفاع والمخابرات والأمن القومي والأمن العام ، والتي توجد لدى الجهات المسموح لها بتجميع وحفظ البيانات الخاصة بمصالح الدولة العليا وأمنها .

ففي بريطانيا مثلاً نص قانون حماية المعلومات الصادر عام ١٩٨٤ على استثناء هام يرد على حق الفرد في الاطلاع ، ويتمثل ذلك في حالة السرية التي تقتضيها مصلحة الأمن القومي . ولقد انتقد هذا النهج ، انطلاقاً من انه إذا كان ولا بد من مثل هذا المنع ، فلا اقل أن يصار إلى إيجاد هيئة رقابية لها الحق في الاطلاع حتى لا يساء استخدام المعلومات ، وتجدر الإشارة هنا إلى أن هذه الهيئة قد وجدت فعلاً منذ عام ١٩٨٤ ، بإنشاء هيئة حماية المعلومات، حيث يسمح للفرد عن طريق هذه الهيئة بالاطلاع بطريق مباشر على البيانات والمعلومات المتعلقة به وان يحصل على مستخرج لنفسه ، وان يصحح البيانات والمعلومات الخاطئة ويعدلها<sup>(١)</sup> .

أما في التشريع الفرنسي فان القانون الصادر بشأن المعلوماتية والحريات ذهب إلى عدم حرمان الشخص من حق الاطلاع على هذه البيانات ، ولكن لم يجعل الاطلاع مباشراً عن طريق الشخص نفسه ، وانما يكون غير مباشر إذ يجب ان يوجه الشخص طلبه إلى الجهة الإدارية المختصة بالإشراف على تطبيق القانون ، أي اللجنة القومية للمعلوماتية والحريات، والتي تقوم بدورها بندب أحد أعضائها من القضاة الحاليين أو السابقين ، حيث تقوم بإجراء التحريات اللازمة والاطلاع ، كما له أن يقوم بالتعديلات

(١) Lan Loyd "the Data Protection Act \_ Little Brother Fights Back" in modern Law

Review Vol . 48 March 1985 , P . 191 -192

نقلا عن / المقاطع ، المرجع نفسه ، ص ١١٢

والتصحیحات إذا كان هناك مقتضى لذلك . ثم تقوم اللجنة بعد ذلك بأخطار صاحب الشأن بان التحقق وإجراء اللازم قد تم<sup>(٢)</sup> .

ومن الجدير بالذكر هنا أن النص يسري على الاطلاع بشأن هذه النوعية من المعلومات بصرف النظر عن الجهة القائمة على بنوك المعلومات ، فالعبارة بطبيعة المعلومات، وتختص الجهة الإدارية بتحديد طبيعة المعلومات وبالتالي ما إذا كان الاطلاع مباشراً أو غير مباشر ، وإذا كانت المعلومات المختزنة مختلفة فان ما يتعلق منها فقط بالأمن القومي والأمن العام يكون الاطلاع عليه غير مباشر ، أما المعلومات الأخرى فيكون الاطلاع عليها بشكل مباشر . ولذلك لا يجوز اطلاع صاحب الشأن على المعلومات المتعلقة بالأمن القومي والأمن العام وإنما يقوم القاضي المنتدب بالاطلاع عليها وإجراء التحريات للتأكد من صحتها ، وإدخال ما يكون مناسباً من تصحيحات .

غير انه لا يجوز إبلاغ الشخص بهذه المعلومات لان ذلك يمس الأمن حيث قد يضر بما يكون جارياً من تحريات ومتابعة لانشطة معينة ، ولهذا يذهب بعض الفقه<sup>(٣)</sup> المقارن - بحق - إلى أننا بصدد رقابة على البيانات أكثر من ممارسة حق الاطلاع .

## ٢ . الاطلاع على المعلومات الطبية :

يخضع حق الاطلاع أو الاتصال بالمعلومات الطبية المتعلقة بالشخص إلى قواعد خاصة لذا فانه لا يجوز اطلاع المريض مباشرة على المعلومات المتعلقة بحالته الصحية ، وإنما يجوز فقط للطبيب الذي يحدده المريض الاطلاع على المعلومات ، ويقوم الطبيب باطلاع المريض على هذه المعلومات وفقاً للقواعد العامة في العلاقة ما بين الطبيب والمريض ووفقاً لأخلاقيات مهنة الطب .

وعلى اثر ذلك يكون الاطلاع غير مباشر بواسطة الطبيب ، والهدف من ذلك هو الحفاظ على مصلحة المريض حيث قد يحصل على معلومات طبية لا يستطيع ان يدرك معناها ، ولهذا فان حصوله عليها يجب ان يكون من خلال من يبصره في لغة مفهومه له بضمنون هذه المعلومات ، ولكي لا تكون مصدراً لخوف المريض واضطرابه في

(٢) الاخواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الالكتروني ، مرجع سابق ، ص ٥٣ .  
(٣) مايسل ، التشريع الفرنسي واتجاهات القضاء المتعلقة بحماية المعلومات الشخصية ، المجلة الدولية للقانون المقارن ، ١٩٨٧ ، ص ٥٧٥ . نقلاً عن /الاخواني ، المرجع السابق ، ص ٥٣-٥٤ .



الوقت الذي يدري فيه بحقيقتها ، وتبدو خطورة ذلك على المريض إذا كان يعالج من اضطراب أو مرض نفسي أو عقلي.

ويلاحظ أخيراً ان هذا القيد لا يسري إلا على حق الاطلاع فقط ، فلا يجوز أعماله بالنسبة لاحق في التصحيح حيث يستطيع ان يقوم به مباشرة ، وذلك بعد العلم من الطبيب بمضمون المعلومات .

ومن الجدير بالذكر ان المشرع الاردني لم يجرم الاطلاع المجرد على المعلومات الخاصة لا في قانون العقوبات ولا في اي قانون اخر حيث يرجع السبب في ذلك - برأي احد الفقهاء - الى عدم تحقق الضرر جراء هذا السلوك <sup>(١)</sup>.

ونتفق مع من يرى " ان قانون العقوبات الاردني لم يواكب الاشكال الجرمية المستحدثة في هذا الجانب فلا نلمس نص في هذا القانون يجرم افعال الاختراق لانظمة المعلومات ولا الدخول غير المشروع الى الانظمة ، ولا البقاء في النظام حال الدخول اليه بطريق الصدفة ... الخ ، مما يعني ان اي من الاعمال المحظورة من هذا القبيل يمكن ان يؤدي الى افلات الجاني من مطرقة العقاب" <sup>(٢)</sup> .

(١) المناعسة ، جرائم الحاسوب الالي والانترنت ، مرجع سابق ، ص ٢٢٠ .  
(٢) الدلالة ، مشكلات الحق في الخصوصية في ظل الاستخدامات اللامنهجية لبنوك المعلومات ، مرجع سابق ، ص ٢٠-٢١ .

## المطلب الثاني

### الحق في تصحيح المعلومات

يعتبر حق الفرد بتصحيح المعلومات وتعديل البيانات من الضمانات الهامة التي لا بد وان تعطى للفرد ما دام أن هناك معلومات مخزنة عنه آلياً لدى بنوك المعلومات، حفظاً لحقه في حماية معلوماته الشخصية.

يحق للفرد الذي يعلم بان هناك معلومات مخزنة عنه لدى الاجهزة الحكومية او الخاصة، وقام بالاطلاع على هذه المعلومات او حصل على نسخة منها ، ان يطلب من الحائز لتلك المعلومات المتعلقة به ، تصحيح وتعديل ما يشوبها من اخطاء لكي يتوافق مع الحقيقة لئلا يوقع به اضراراً قد تؤثر على مركزه لدى جمهور المتعاملين معه ، مما يؤثر على سمعته ويسبب له خسائر لا سبيل لتجنبها<sup>(١)</sup> .

ومن هنا فانه لا بد وان "يعطى الفرد حقه في التصويب والتعديل للمعلومات في وقت مبكر، وقبل أن يضار منها ، إذ أن في تأخير الفرد من ممارسة هذا الحق إلى ما بعد وقوع الضرر ، ما يضطره لا محالة من اللجوء إلى استخدام أحد أساليب الحماية العلاجية اللاحقة، مثل طلب التعويض عما أصابه من ضرر"<sup>(٢)</sup> . لذا فان الحق يدخل في إطار الإجراءات الوقائية التي تستهدف في المقام الأول تفادي حدوث أضرار نتيجة وجود معلومات خاطئة ، ولذلك يعد الحق في التصحيح من إجراءات الحماية الوقائية الشخصية .

فمن المبادئ الأساسية في مجال المعلوماتية أن الجهة القائمة على بنوك المعلومات تلتزم بمراعاة صحة ودقة المعلومات المخترنة وان تقوم بصفة دورية بتقحيح المعلومات بما يجعلها متفقة مع الحقيقية ، كما ينبغي عليها أن تلتزم بالتحري عن جدية ودقة المعلومات التي تتلقاها وتسجلها ، وتنعقد مسؤوليتها في أحوال سوء التحريات أو الاعتماد على وثائق وبيانات مشكوك فيها ، أو في حالة سوء عمليات البرمجة ومما يؤيد التشدد في مسؤوليتها أنها تستهدف الحصول على الربح من بيع

(١) المقاطع ، حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ١١٣ ، ١١٤ .

(٢) المرجع نفسه ، ص ١١٣ .

المعلومات ، فيجب أن يكون الحصول على المعلومات وتخزينها قد تم بناء على إجراءات معقولة وإلا توافر عنصر الخطأ في جانب الجهة القائمة على هذه البنوك<sup>(١)</sup> .

وإذا تحقق للشخص ضرر بسبب هذه المعلومات الخاطئة وغير الدقيقة ، فإن له الحق في الحصول على تعويض لجبر الضرر طبقاً للقواعد العامة في المسؤولية المدنية .

وينص القانون الفرنسي بشأن المعلوماتية والحريات<sup>(٢)</sup> على منح الشخص الحق في تصحيح وتكملة وإيضاح وتنقيح أو محو المعلومات المتعلقة به إذا كانت تلك المعلومات غير صحيحة ، أو ناقصة أو تغيرت أو غامضة ، وكذلك الحق في محو المعلومات التي يكون الحصول عليها أو استخدامها أو الاحتفاظ بها غير مشروع وفقاً لما يقرره القانون .

والمشكلة الرئيسية التي تثور في مجال استعمال حق التصحيح تتعلق بتحديد من الذي يقع على عاتقه عبء الإثبات : هل هو الشخص طالب التصحيح حيث يلتزم بإثبات عدم صحة البيانات أم الجهة القائمة على بنوك المعلومات حيث تلتزم على العكس بإثبات صحة البيانات ؟ .

يتجه القانون المقارن إلى الخروج على القواعد العامة في الإثبات ، وإلقاء عبء الإثبات على عاتق الجهة القائمة على بنوك المعلومات ، وذلك فيما عدا حالة واحدة وهي المتعلقة بالحصول على المعلومات من الشخص نفسه صاحب هذه المعلومات ، ويرجع السبب من قلب عبء الإثبات إلى حماية الشخص بإعطاء حق التصحيح دفعة قوية مما يجعله أكثر فاعلية<sup>(٣)</sup> .

والشخص الذي يملك الحق في طلب التصحيح هو نفسه الذي يحق له الاطلاع والحصول على مستخرج من المعلومات ، أما بالنسبة لأحوال الاطلاع غير المباشر فإن الحق في طلب التصحيح يكون فقط للأشخاص الذين يخولهم القانون حق الاطلاع ، وذلك لان الشخص المتعلقة به المعلومات قد لا يطلع عليها إطلاقاً كما هو الحال بالنسبة

(١) حسبو ، حماية الحريات في مواجهة نظم المعلومات ، مرجع سابق ، ص ١٤٧ .  
(٢) المادة (٣٦) من القانون الفرنسي بشأن المعلوماتية . نقلاً عن /د. الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني ، مرجع سابق ، ص ٥٥ .  
(٣) انسل ، في تطبيق القواعد العامة في الإثبات : كتاب حماية المعلومات الشخصية في القانون العام السويسري ، المجلة الدولية للقانون المقارن ، سنة ١٩٨٧ ، ص ٦٠٠ ، مشار إليه لدى /د. الاهواني ، المرجع نفسه ، ص ٥٦ .

للمعلومات المتعلقة بأمن الدولة والأمن العام ، وقد لا يطلع عليها أحيانا إذا رأى الطبيب مثلاً عدم اطلاع المريض على المعلومات ، أما إذا أطلع عليه عليها جاز للمريض إجراء التصحيح .

فالحماية القانونية للشخص في مواجهة بنوك المعلومات تعتبر مجرد امتداد للقواعد العامة في حماية الحقوق اللصيقة بالشخص ، فهذه القواعد تهدف إلى حماية حقوقه الشخصية في مواجهة مخاطر هذه البنوك ، فالقانون اقر حماية خصوصية الأفراد وفاعلية تلك الحماية لا تكتمل إلا بتوفير سبل الحماية المناسبة للمخاطر التي تتهددها . فموضوع الحماية ليس المعلومات المخزنة وإنما المصالح التي تتهددها هذه المعلومات غير الصحيحة<sup>(١)</sup> .

ومن المعلوم لدينا انه إذا كانت المعلومات التي أخذت عن الأفراد ناقصة أو غامضة أو خاطئة، فإن الجهة القائمة على بنوك المعلومات تلتزم بإجراء التصحيح المناسب دون حاجة لان يقدم صاحب الشأن ما يثبت ان له مصلحة في ذلك ، ولا غرو أن لهذه الجهة مصلحة في إجراء التصحيح لكي تكون معلوماتها صحيحة مما يعزز مصداقيتها .

ويجوز لصاحب الشأن ان يطلب محو البيانات التي تم الحصول عليها بطريقة غير مشروعة ، مثل تسجيل البيانات المحذور تسجيلها أو التي تم الحصول عليها بوسائل احتيالية.

وفي التشريع الأردني لم نجد نصاً واحداً يعطي الفرد الحق في تصحيح المعلومات التي أخذت عنه وتصويبها في مواجهة بنوك المعلومات ، حيث ان المشرع الجزائي الأردني لم يتدخل إلى الآن لسن تشريع خاص في مواجهة أي اعتداء قد يقع على المعلومات الخاصة بالأفراد ، والتي من شأنها ان تهدد المصالح المختلفة لهم ، وتدع المجال مفتوحاً للانتهاكات المتعددة للحق في الخصوصية ، إلا أن الشخص الذي يضر من مثل هذه المعلومات الخاطئة التي أخذت عنه عليه أن يلجأ إلى القواعد العامة في القانون المدني لجبر الضرر الذي لحق به، والتعويض عما أصابه من خسارة نتيجة نسبة معلومات خاطئة إليه ، جعلته في موضع حرج وازدراء أمام الآخرين .

(١) حسبو ، حماية الحريات في مواجهة نظم المعلومات ، مرجع سابق ، ص ١٥١ .

وعلى النقيض من ذلك نجد ان المشرع الفرنسي قد افرد و سن تشريع خاص في مواجهة أي اعتداء قد يقع على الأشخاص من قبل بنوك المعلومات والحاسبات الإلكترونية ، حيث فرض المشرع حماية جنائية للبيانات الشخصية في مواجهة نظم المعلومات وذلك في القانون الصادر في ٦ يناير ١٩٧٨ والمسمى بقانون نظم المعالجة الرقمية والحرية ، حيث يهدف هذا القانون إلى تحقيق التوازن ما بين الاستخدام الحر والكامل للمعلوماتية من ناحية ولحماية المواطن في إطار نظام ديمقراطي حر من ناحية أخرى .

ويتطلب القانون ضرورة أخطار اللجنة الوطنية للمعلوماتية والحريات<sup>(٢)</sup> عند معالجة أي بيانات شخصية من قبل أشخاص القانون الخاص ، أو الحصول على تصريح مسبق منها ، إذا كان من يقوم بجمع المعلومات أحد أشخاص القانون العام أو أحد أشخاص القانون الخاص العاملين لحساب الدولة<sup>(١)</sup> .

لذلك يتعين على القائمين على بنوك المعلومات أخطار اللجنة الوطنية للمعلوماتية والحريات، إذا ما أرادوا التعامل مع البيانات الشخصية ، والتي قد يؤدي نشرها إلى التقاطها أو تزيفها والاستيلاء عليها ، لذا تفرض اللجنة ضرورة أخطار المواطنين بالمخاطر المترتبة على وضع بياناتهم الشخصية ، وحقهم في الاعتراض على نشر هذه البيانات في أي وقت ، بالإضافة إلى حقهم في الاطلاع على هذه البيانات وتصحيحها أو محوها وفقاً لاسباب مشروع<sup>(٢)</sup> .

(٢) مهمة هذه اللجنة مراقبة احترام القانون لدى كل الأشخاص المتصلين بتطبيق أحكامه ، ولها سلطة اتخاذ القرارات اللازمة لذلك ، ويلتزم أعضاؤها بالمحافظة على الأسرار التي يمكنهم العلم بها بحكم وظيفتهم وفقاً للمادة

(١٣-١٠) من قانون العقوبات الفرنسي الجديد المعمول به سنة ١٩٩٤ ، كما تختص بإصدار الترخيص السابق = = من اجل إنشاء نظم المعلومات أو تلقي الإخطارات من الأشخاص في هذا الخصوص ، وكذلك تقوم بالرقابة اللاحقة على إنشاء نظم المعلومات .

للمزيد انظر : د. عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، الطبعة الثانية ، دار النهضة العربية، القاهرة ، ١٩٩٥ ، ص ٥٦ . وكذلك د. عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الإلكترونية ( الكتاب الأول ) ، الطبعة الأولى ، دار الفكر الجامعي الإسكندرية ، ٢٠٠٢ ، ص ٧٠ .

(١) د. مدحت رمضان ، الحماية الجنائية للتجارة الإلكترونية ، دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية، القاهرة ، ٢٠٠١ ، ص ٨٥ .

(٢) نفس المرجع السابق ، ص ٨٦ .

## المطلب الثالث

### الحق في المحافظة على خصوصية المعلومات وسريتها

من المبادئ الأساسية أن تخزين المعلومات لا يعني أن هذه المعلومات قد انتقلت من الخصوصية إلى العلانية ، كما أن الرضا بالتجميع والتخزين لا يعني حرية تداول ونقل المعلومات إلى الكافة .

وفي التطبيق العملي فإن المعلومات تخزن من أجل استخدامها سواء في النطاق الداخلي أو في النطاق الخارجي . ففي النطاق الداخلي يتم استخدام نظام المعلومات من قبل الجهة المسؤولة عن بنوك المعلومات لأغراضها الداخلية دون أن يدخل في الاستخدام نقل المعلومات للغير ، أما في النطاق الخارجي فالنظام يستهدف تزويد الغير بالمعلومات التي تم تجميعها .

والحق في المحافظة على سرية المعلومات يتوافر في الحالتين من حيث المبدأ ، وإن كان يختلف من حيث المدى أو الصورة التي يكون عليها ، غير أنه في الحالتين يجب المحافظة على خصوصية المعلومات لإتخاذ الإجراءات الكفيلة بمنع تسريبها على خلاف ما يقتضيه التداول المسموح<sup>(١)</sup> .

وليس هناك صعوبة في إلزام الجهة القائمة على بنوك المعلومات بالمحافظة على سرية المعلومات إذا كانت الجهة ملتزمة قانوناً بعدم إفشاء السر، مثل السر الطبي . فالمعلومات الطبية المختزنة في بنوك المعلومات ولدى إحدى المستشفيات لا يجوز إفشائها على خلاف ما يقضي به القانون ، وفي الأحوال التي ينشأ فيها نظام المعلومات طبقاً للقانون فإن المشرع يلزم القائمين على المعلومات بالمحافظة على السرية<sup>(٢)</sup> .

ومن الجدير بالذكر أن المشرع المصري قد نص في المادة (١٣) من قانون الأحوال المدنية رقم (١٤٣) لسنة ١٩٩٤ على أن " تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتي تشتمل على السجلات أو الدفاتر أو

(١) BEER GABEL . Le Controle de l'Administration Par la Commission nationale de l'Informatique des Libertés . R.D.P. -1980 . P . 1051

نقلاً عن / حسب ، حماية الحريات في مواجهة نظم المعلومات ، مرجع سابق ص ١٥٥ .  
(٢) الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني ، مرجع سابق ، ص ٦٢ .

الحاسبات الآلية أو وسائط التخزين الملحقة سرية ، ولا يجوز الاطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون ووفقاً لأحكامه .وتعتبر البيانات أو المعلومات أو الإحصائيات المجمعة التي تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين سرّاً قومياً ، ولا يجوز الاطلاع عليها أو نشرها إلا لمصلحة قومية أو علمية وبإذن كتابي من مدير مصلحة الأحوال المدنية أو من ينيبه وفقاً للأوضاع والشروط التي يحددها القانون واللائحة التنفيذية ... "

ومن خلال النص نلاحظ أن المشرع المصري يفرق بين البيانات السرية ، والبيانات التي تعتبر سرّاً قومياً ، فالمعلومات أو البيانات السرية تتعلق بمواطن محدد ، فتعتبر هذه البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين سرية ، أما السر القومي فهو لا يتعلق ببيان يتصل بمواطن محدد وإنما يتعلق ببيانات أو إحصائيات مجمعة على الحاسبات الآلية أو بنوك المعلومات ، أو وسائط التخزين ، مثل استخلاص إحصائيات عن عدد الذكور والإناث أو عن حالات الزواج والطلاق ، وما يتعلق بالسر القومي لا يجوز الاطلاع عليه أو نشره إلا لمصلحة قومية أو علمية وبإذن كتابي من مدير مصلحة الأحوال المدنية أو من ينيبه.

ولكن الصعوبة تظهر في الأحوال التي لا يتوافر فيها حاله من حالات الالتزام بعدم إفشاء السر طبقاً لنص من نصوص القانون . وفي هذا الخصوص تبدو أهمية وضع قواعد خاصة في مجال نظم المعلومات الآلية ، وتتمثل هذه القواعد في أمرين ، أولهما : عدم نقل أو تداول المعلومات خارج الهدف من إقامة نظام المعلومات ، وثانيهما : وضع ما يلزم القائمين على الحاسب الآلي وبنوك المعلومات بالمحافظة على خصوصية المعلومات<sup>(١)</sup> .

وكذلك حرصت المادة (٦٥) من قانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ على النص على أن تلتزم مصلحة الأحوال المدنية باتخاذ كافة التدابير اللازمة لتأمين البيانات الشخصية المجمعة والمخزنة بالحاسبات الآلية أو بوسائط التخزين الملحقة بها ضد أي اختراق أو عبث أو اطلاع أو إفشاء أو تدمير أو مساس بها بأية صورة كانت في غير الأحوال التي نص عليها القانون.

(١) الاهواني ، حماية خصوصية المعلومات في مواجهة الحاسب الآلي ، مع دراسة خاصة لقانون الأحوال المدنية رقم ٤٣ لسنة ١٩٩٤ ، أبحاث ودراسات المؤتمر العلمي الثالث لنظم المعلومات وتكنولوجيا الحاسبات المنعقد في القاهرة في الفترة من ١٢ - ١٤ ديسمبر ١٩٩٥ ، ص ٩٠ .

والالتزام باتخاذ التدابير يقتضي اللجوء إلى الوسائل الفنية اللازمة لتوفير الحماية للمعلومات الشخصية ، وكذلك اتخاذ التدابير الأمنية اللازمة مثل الحراسة وتحديد من يحق لهم الدخول إلى مكان الحاسب الآلي وبنوك المعلومات وإجراءات التحقق من شخصيتهم .

ويلاحظ أن المادة (٦٥) من القانون قد حددت على سبيل المثال وليس الحصر صور المساس بالمعلومات الشخصية ، ولقد تضمنت المادة (٧٤) من ذات القانون صوراً أخرى للمساس ، إذا تنص هذه المادة على انه " يعاقب بالحبس مدة لا تتجاوز ستة اشهر وبغرامة لا تزيد على خمسمائة جنية أو بإحدى العقوبتين كل من اطلع أو شرع في الاطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقه بها أو قام بتغييرها بالإضافة أو الحذف أو بالإلغاء أو بالتدمير أو بالمساس بأي صورة من الصور أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون ووفقاً للإجراءات المنصوص عليها فيه ، فإذا وقعت الجريمة على البيانات والمعلومات أو الإحصاءات المجمعة تكون العقوبة هي السجن ... " .

أما فيما يتعلق بالحق في المحافظة على خصوصية المعلومات وسريتها في التشريع الأردني فيمكننا حماية البيانات الشخصية من خلال قانون الأحوال المدنية ، وقانون الإحصاءات العامة ، وقانون ضمان حق الحصول على المعلومات ، وذلك في ثلاثة فروع مستقلة وعلى النحو الآتي :-

الفرع الاول : حماية البيانات الشخصية في ظل قانون الأحوال المدنية رقم ٩ لسنة ٢٠٠١ .

تنص المادة (٧) من هذا القانون على سرية البيانات والمعلومات المسجلة لدى السجلات الخاصة بدوائر الأحوال المدنية ، حيث تنص الفقرة (أ) من هذه المادة على " لا يجوز نقل أي من السجلات المنصوص عليها في الفقرة (ب) من المادة (٤) (١) من هذا القانون خارج المكتب ، وتعتبر البيانات الواردة في هذه السجلات سرية .

(١) الفقرة (ب) من المادة (٤) تنص على :- يعد في كل مكتب :



نلاحظ في هذا النص أن المشرع الأردني اسبغ على هذه البيانات المتعلقة بالأشخاص من حيث واقعات الولادة والزواج والطلاق وجميع القيود والوثائق المتعلقة بأصول الشخص أو فروعه صفة السرية ، لما لها من خصوصية معينة .

ومن الجدير بالذكر انه عند مقارنة نص المادة (٤) والمادة (٧) من قانون الأحوال المدنية الأردني ، بنصوص المواد (١٣ ، ٦٥ ، ٧٤) من قانون الأحوال المدنية المصري ، نرى أن نص المادة (١٣) من القانون المصري كانت واضحة وشاملة وتشتمل على جميع الوسائل التي يمكن تخزين المعلومات عليها ، كما اعتبر أن جميع البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين سرية لا يجوز الاطلاع عليها ، أو الحصول على بياناتها، إلا في الحالات التي ينص عليها القانون .

أما فيما يتعلق باتخاذ كافة التدابير والاحتياطات اللازمة لتأمين البيانات الشخصية المجمعة والمخزنة في الحاسبات أو وسائط التخزين الأخرى ، ضد أي اختراق أو عبث أو اطلاع غير مبرر ، فإن المادة (٦٥) قد نصت على مثل هذا الأمر ، وذلك ضماناً للشخص في السيطرة على معلوماته وحقاً له في المحافظة على خصوصية معلوماته وسريتها ، وكذلك بالنسبة للمادة (٧٤) من ذات القانون والتي وسعت من صور المساس بالمعلومات الشخصية المخزنة لدى أجهزة بنوك المعلومات من حيث الإفشاء أو الحذف أو التدمير ، أو إلغاء البيانات ، كما بينت العقوبة وهي الحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين.

وعند قراءة نصوص قانون الأحوال المدنية الأردني وتفحصها فأدنا لا نجد مثل هذا النص كما هو في القانون المصري والذي يتخذ كافة الاحتياطات اللازمة من اجل المحافظة على المعلومات الشخصية للأفراد من عبث الآخرين ، وهذا يعتبر قصور في التشريع الأردني ، نتمنى ان يتم تداركه من قبل المشرع .

ومن الملاحظ أن المشرع الأردني في هذا القانون لم يضع عقوبة معينة على أي إفشاء أو اطلاع غير مبرر للبيانات الواردة في هذه السجلات كما فعل المشرع المصري ، وانما ترك ذلك للقواعد العامة المتعلقة بإفشاء الأسرار في قانون العقوبات الأردني ، وخاصة المادة (٣٥٥) والتي تعاقب بالحبس لمدة لا تزيد على ثلاث سنوات .

١. سجل الحاسب الآلي .  
٢. أي سجل آخر يقرره المدير .

الفرع الثاني : حماية البيانات الشخصية في ظل قانون الإحصاءات العامة المؤقت  
رقم (٨) لسنة ٢٠٠٣ :-

أسبغ المشرع الاردني السرية على المعلومات والبيانات الإفرادية التي تجمع  
لأغراض التعداد والإحصاءات السكانية بنصه في المادة (١١) على انه :

أ. تعتبر سرية المعلومات والبيانات الإفرادية التي تقدم للدائرة والمتعلقة  
بأي مسح أو تعداد ولا يجوز لها أو لأي من العاملين لديها ، تحت طائلة المسؤولية  
القانونية ، اطلاع أي شخص أو جهة عامة أو خاصة عليها أو الكشف عنها ، كليا أو  
جزئياً ، أو استخدامها لأي غرض غير أعداد الجداول الإحصائية .

ب. تتقيد الدائرة عند نشرها للإحصاءات الرسمية بعدم إظهار أي بيانات  
افرادية حفاظاً على سريتها .

ج. يتعين على كل موظف في الدائرة أداء القسم والتوقيع على تعهد يلتزم  
بموجبه بعدم إفشاء أو نشر أي معلومات أو بيانات افرادية .

د. على الدائرة اتخاذ الإجراءات الكفيلة بحماية البيانات التي تم جمعها وحفظها  
في أماكن تتوفر فيها شروط الأمان والسلامة .

فالمشرع الأردني بهذا النص أراد أن يضيف حمايته على المعلومات الشخصية  
التي تؤخذ عن الأفراد ، وأسبغ عليها صفة السرية لما لها من خصوصية معينة ،  
وحسناً فعل المشرع عندما ألزم العاملين في الإحصاءات العامة تحت طائلة المسؤولية  
القانونية بعدم اطلاع أي شخص أو جهة عامة أو خاصة ، سواء كانت مؤسسات  
حكومية أو مؤسسات خاصة على البيانات المتعلقة بالأفراد، كما ألزم الموظف في  
الدائرة بعدم إفشاء أو نشر أي معلومات أو بيانات إفرادية .

وتجدر الإشارة هنا أن الفرد هو الذي قام بإعطاء هذه المعلومات طوعاً أي  
برضاه وبالتالي يفترض أن تكون هذه البيانات التي أعطيت صحيحة ابتداءً ، وعليه فإن  
الفرد كضمانة أساسية قد سيطر على معلوماته الشخصية ، وان جميع المعلومات التي  
تم تسجيلها لدى دائرة الإحصاءات العامة صحيحة ، إلا إذا كانت هناك أخطاء مهنية  
نتيجة إدخال هذه البيانات إلى أجهزة الحاسب الإلكتروني وأجهزة بنوك المعلومات .

وعلى هذا الأساس فأدنا لم نجد أن للشخص الحق في الوصول إلي هذه المعلومات وتصحيح ما هو خاطئ منها نتيجة خطأ في الجهاز ، فالأخطاء التقنية محتملة الوقوع ، إذ أن نسبه معلومات معينة إلى شخص ما قد تؤثر على سمعته في حالة إذا ما تم تسرب هذه المعلومات أو إفشاؤها بطريقة غير مشروعة .

وكما يبدو من نص الفقرة (د) من نفس المادة أن المشرع ألزم الدائرة باتخاذ كافة الإجراءات والتدابير الكفيلة بحماية البيانات التي تم جمعها وحفظها في أماكن تتوافر فيها شروط الأمان والسلامة خوفاً من ضياع هذه البيانات أو تسربها إلي الغير ، الذي قد يكون له مصلحة في ذلك سواء كان شخصاً عادياً أو مؤسسة خاصة أو شركة تجارية .

وفي الواقع العملي فإن إجراءات الأمان والحماية تتكون من شقين رئيسيين :-  
الأول :- الشق الفني :<sup>(١)</sup>

ويشمل الإجراءات الفنية المتعلقة بالشفرة الخاصة بمستخدم الحاسب ( الكود ) ، والتي تتيح له الدخول إلى الحاسب واستخدامه . وهذا الشق لا يوفر حماية إلا في حدود ٢٠% .

الثاني : ويتعلق بحسن التنظيم الإداري والفني للجهة القائمة على الحاسب الآلي كبنك للمعلومات ، بل ويشمل أيضا موقع ومواصفات البناء الذي وضع به الحاسب الآلي<sup>(٢)</sup> .

والقصد من إجراءات الأمان هو الحفاظ على سرية وخصوصية المعلومات من ناحية والتأكيد على احترام المبادئ التي يقوم عليها القانون من ناحية أخرى .

وترصد المادة (١٥) من ذات القانون عقوبة الحبس مدة لا تقل عن ستة اشهر ولا تزيد على سنة أو بغرامة لا تقل عن خمسمائة دينار ولا تزيد على ألف دينار أو بكلتا العقوبتين لـ : ١. أي موظف في الدائرة قام بإفشاء أي معلومات أو بيانات إحصائية سرية بالمعنى المنصوص عليه في المادة (١١) من هذا القانون أو سر من

(١) حسبو ، حماية الحريات في مواجهة نظم المعلومات ، مرجع سابق ، ص ١٦١ .  
(٢) الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني ، مرجع سابق ، ص ٦٥-٦٦ .

أسرار الصناعة أو التجارة وغير ذلك من أساليب العمل التي تعتبر من أسرارها ويكون قد اطلع عليها بحكم عمله .

٢. تعتمد الاحتفاظ بأي وثائق إحصائية تحتوي على البيانات او تعتمد إتلافها أو تزويرها .

٣. إضاعة أي وثائق إحصائية لها صفة سرية تحتوي على البيانات بسبب الإهمال.

الفرع الثالث :- حماية البيانات الشخصية في ظل قانون ضمان حق

الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧

صدر مؤخراً في الاردن قانون ضمان حق الحصول على المعلومات رقم (٤٧)

لسنة ٢٠٠٧ الذي بدأ نفاذه بتاريخ ٢٠٠٧/٦/١٧ ، حيث يعتبر هذا القانون من القوانين التي تنظم كيفية الحصول على المعلومات بالنسبة لطالب هذه المعلومة ، سواء كان مؤسسات او افراد عاديين .

وبموجب هذا القانون تم تشكيل مجلس المعلومات حسب نص المادة (٣)(١) فقرة (أ) حيث يتولى هذا المجلس ، مجموعة من المهام والصلاحيات حسب نص المادة (٤) منها :-

١. ضمان تزويد المعلومات الى طالبيها في حدود هذا القانون  
٢. اصدار النشرات والقيام بالانشطة المناسبة لشرح وتعزيز ثقافة الحق في المعرفة وفي الحصول على المعلومات .  
ومن الملاحظ ان هذا القانون لم يحم المعلومات الشخصية للأفراد من مخاطر التكنولوجيا الحديثة وخاصة بنوك المعلومات وانما جاء لينظم كيفية الحصول على المعلومة، حيث انه الزم كل دائرة ان تقوم بفهرسة وتنظيم المعلومات والوثائق التي تتوافر لديها حسب الاصول المهنية والفنية (٢).

وعرف المشرع في المادة (٣) من هذا القانون الدائرة بانها الوزارة او الدائرة او الهيئة او اي مؤسسة عامة او مؤسسة رسمية عامة او الشركة التي تتولى ادارة مرفق عام.

ويلاحظ على ذلك ان المشرع الاردني قصر تنظيم المعلومات ضمن الدوائر والمؤسسات الحكومية التي تقوم بادارة مرفق عام فقط ، ولم ينظم المعلومات في المؤسسات والشركات الخاصة ، حيث ان هناك مجموعة كبيرة من الشركات والمؤسسات الخاصة لديها كم هائل من المعلومات الشخصية عن الافراد ، مثل شركات التأمين والشركات التي تعنى بشؤون الافراد ، وهذا يعتبر قصور في التشريع الاردني نتمنى على المشرع تداركه.

ومهما يكن من امر فان هذا القانون يعتبر خطوة ايجابية ، حيث انه وضع حجر الاساس في كيفية الحصول على المعلومة بالطرق المشروعة ولاسباب مشروعة .

(١) تنص المادة (٣) فقرة (أ) من قانون ضمان حق الحصول على المعلومات الاردني على :-  
يؤلف بموجب هذا القانون مجلس يسمى ( مجلس المعلومات ) وبشكل على النحو التالي :-

١. وزير الثقافة رئيساً

٢. مفوض المعلومات - نائباً للرئيس

وعضوية كل من : امين عام وزارة العدل ، امين عام وزارة الداخلية ، امين عام المجلس الاعلى للاعلام ، مدير عام دائرة الاحصاءات العامة ، مدير عام مركز تكنولوجيا المعلومات الوطني ، مدير التوجيه المعنوي في القوات المسلحة ، المفوض العام لحقوق الانسان .

(٢) المادة (٤) فقرة (أ) تنص على " على كل دائرة ان تقوم بفهرسة وتنظيم المعلومات والوثائق التي تتوافر لديها حسب الاصول المهنية والفنية المرعية وتصنيف ما يتوجب اعتباره سرياً ومحماً حسب التشريعات النافذة خلال مدة لا تتجاوز ثلاثة اشهر من تاريخ نشر هذا القانون في الجريدة الرسمية " .

وهذا ينسجم مع المادة (٧) من القانون ، حيث انه لكل اردني الحق في الحصول على المعلومات التي يطلبها وفقاً لاحكام هذا القانون اذا كانت له مصلحة مشروعة او سبب مشروع .

تنص المادة (١٠) من هذا القانون على أنه " لا يجوز طلب المعلومات التي تحمل طابع التمييز الديني أو العنصري أو العرقي أو التمييز بسبب الجنس أو اللون . "

وحسناً فعل المشرع من خلال هذا النص ، حيث أن أي معلومة تتعلق بالإنتماءات الدينية او العرقية او العنصرية يجب أن تكون محمية ولا يجوز الكشف عنها في أي حال من الأحوال ، فعدم الكشف عن مثل هذه المعلومات هو حماية لها ، وعدم إطلاع الاخرين على مثل هذه المعلومات .

إن ما يهمننا في هذا القانون هو المادة (١٣) فقرة (هـ) حيث تنص على أنه " مع مراعاة أحكام التشريعات النافذة ، على المسؤول أن يمتنع عن الكشف عن المعلومات والملفات الشخصية المتعلقة بسجلات الأشخاص التعليمية أو الطبية أو السجلات الوظيفية أو الحسابات أو التحويلات المصرفية أو الأسرار المهنية " .

نلاحظ من خلال النص أن المشرع في هذا القانون قد أكد على حماية المعلومات الشخصية للأفراد خاصة ما يتعلق منها بسجلات الاشخاص التعليمية أو الطبية أو الوظيفية والزم المسؤول أن يمتنع عن الكشف عنها لأن هذه البيانات أو المعلومات لها صلة مباشرة بالشخص وبالتالي فإن أي معلومة تتعلق بالامور السابقة إذا تم إفشائها أو كشفها للآخرين فإنها قد تسيء إليه .

وتجدر الإشارة هنا الى أن المعلومات التي تتعلق بالسجلات الطبية أو الوظيفية أو الحسابات المصرفية أو الأسرار المهنية هي معلومات محمية بموجب تشريعات أخرى

(( التشريعات الخاصة لحماية الأسرار )) ، ولكن هذا القانون جاء ليؤكد على أن مثل هذه المعلومات لا يجوز الكشف عنها أو الحصول عليها ، وبالتالي على المسؤول عندما يقدم إليه طلب الحصول على المعلومات أن يمتنع عن تقديم أو إعطاء مثل هذه المعلومات السرية أو الخاصة .

فكل دائرة تقوم بتنظيم المعلومات التي لديها وتصنيف ما يتوجب اعتباره منها سرياً ومحماً بموجب التشريعات النافذة ، حيث تنحصر مسؤولية مفوض المعلومات القانونية فيما يتعلق بالمعلومات المحفوظة في دائرته<sup>(١)</sup> .

كما أن المشرع في هذا القانون لم ينص على عقوبة معينة على المسؤول إذا قام بالكشف عن المعلومات ذات الصبغة السرية والخاصة بالأفراد ، وإنما ترك ذلك للقواعد العامة في قانون العقوبات بصريح المادة ( ٣٥٥ ) منه .

### المطلب الرابع

#### الحق في تأقيت المعلومات واستردادها ومحوها وإلغائها

تعتبر ضمانات التأقيت من الحقوق المهمة التي تسعف الفرد في أن يهنا بحدية طيبة، دون أن يكون قلق البال ولفترة قد تمتد طوال حياته، هو ضرورة وضع مدة محددة، يجوز أثنائها فقط للحائز على المعلومات المتعلقة بهذا الفرد أن يحتفظ بها، أي أنه لا يجوز له أن يبقى حائزاً لمثل هذه المعلومات عن الفرد لمدة غير محددة.

والحق في تأقيت المعلومات يستوجب أمرين ، الأول: هو أن يحدد مع غرض الاستخدام المدة المتوقع أن تنتهي فيها الحاجة لمثل هذه المعلومات والتي ستلغى بشكل تلقائي ويخطر هذا الفرد بانتهاء وجود مثل هذه المعلومات عنه، أما الأمر الثاني: فهو أن الفرد يحق له أن يطالب هذه الجهات بإنهاء حيازتها للمعلومات التي لديها آلياً عنه، بعد انتهاء الغرض أو الهدف الذي وافق من أجله على إعطائها مثل هذه المعلومات<sup>(١)</sup>.

ومن الجدير بالذكر أن الاتفاقية الأوروبية لحماية المعلومات قد أقرت هذا الحق على أنه أحد الضمانات التي تحمي بواسطتها خصوصية معلومات الأفراد.

(١) المادة (١٥) تنص على "عند تولي مدير عام دائرة المكتبة الوطنية مهام مفوض المعلومات بالإضافة لوظيفته تنحصر مسؤوليته القانونية فيما يتعلق بالمعلومات المحفوظة في دائرته " .

(١) المقاطع، حماية الحياة الخاصة للأفراد وضمائنها في مواجهة الحاسوب الآلي، مرجع سابق، ص ١١٦

كما أن القانون الفرنسي بشأن المعلوماتية والحريات وفي المادة (٢٨) منه ينص على أنه (( لا يجوز الاحتفاظ بالمعلومات الاسمية إلا للمدة المحدودة في طلب إقامة نظم المعلومات أو لمدة تزيد عن المدة اللازمة لتحقيق الغرض من تجميع البيانات واحتياجات البرنامج، إلا إذا سمحت اللجنة القومية للمعلوماتية والحريات بالاحتفاظ بالمعلومات أكثر من المدة المحددة)).

أما فيما يتعلق بالحق في استرداد المعلومات، فهو أن يُعطى الفرد القدرة في أن يسترد ما سبق وان أعطاه من معلومات عن نفسه للغير، سواء تمثل ذلك في شكل معلومات حفظت آلياً عن الشخص، أو كانت في اي صورة من صور المعلومات التي يحتفظ بها عن الشخص، كالآراء والصوت والصورة، أو حتى المعلومات المخزنة في سجلات مقروءة أو مسموعة أو مرئية بناءً على موافقته، فالإنسان الذي وافق على وضع اسمه ضمن دليل أسماء المشتركين في الهواتف له الحق في أن يسترد ذلك مع تحمل التكلفة التي قد تنتج عن ذلك، وهو ثمن إلغاء التخزين الآلي لهذه المعلومات مثلاً، وقد يكون من مصلحة شخص قام في وقت ما بإعطاء معلومات عنه وعن عائلته مثلاً، كنموذج للعائلة الناجحة، مقابل حصوله على تعويض مالي، ثم وجد أن مثل تلك المعلومات التي ستنتشر على الملأ عنه تضر به وتسيء إلى سمعته، فله أن يطالب باسترداد مثل هذه المعلومات مقابل إعادة ما حصل عليه من مقابل مالي، بل وتعويض الجهة التي قبلت ذلك منه عما يكون قد لحقها من ضرر، وهذا الأمر إذا ما حدث حوله خلاف، فإن قاضي الموضوع هو الذي سيبت فيه، ويحدد الضرر ومقدار التعويض اللازم<sup>(١)</sup>.

قد يتعرض الفرد لجملة من المخاطر والمضار نتيجة لوجود معلومات مخزنة عنه آلياً كثيرة ومتنوعة، لذلك فإن الفرد يُعطي ضمانات هامة لايقاف مثل تلك المضار نتيجة وجود مثل تلك المعلومات عنه، من هنا فإن للفرد الحق في أن يمحو البيانات الخاطئة الموجودة عنه، أو التي لم يعد لوجودها داع مما قد يؤدي إلى تحقيق مضار محققة على مصالحه وحقوقه<sup>(٢)</sup>.

(١) المقاطع، حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسوب الآلي ، مرجع سابق ، ص ١١٨ .

(٢) المرجع نفسه ، ص ١١٨-١١٩ .



ومن التطبيقات القضائية التي حدثت في هذا الشأن قضية (Menrad)<sup>(٣)</sup> عام ١٩٧٦ حيث أنها قضية تتعلق بإنشاء ملف قبض مؤقت عن الشخص، فلقد طالب السيد (مينارد) بعد إطلاق سراحه دون أن يدان بأي شيء بمحو المعلومات التي أخذت عنه وقد علق الأستاذ (Shattuck) على هذه القضية منتهياً إلى أنه من المستقر اليوم أنه من حق الفرد في أن يطالب بمحو ملفه (ملف القبض المؤقت) في الأحوال الآتية:

١. عندما يكون القبض مجرد احتجاز مؤقت وليس قبضاً يؤدي إلى سجن مستقر بإدانة قضائية.

٢. عندما يكون القبض قد تم لجريمة بسيطة مثل ازعاج هدوء الناس.

٣. عندما يكون القبض غير دستوري، أو أن تعلن المحكمة لاحقاً عدم دستورية القانون الذي تم القبض استناداً إليه.

وللفرد فضلاً عن محو ملفه، أن يطالب جميع الجهات التي تحتفظ بملفات عنه أن تقوم بإلغاء هذه الملفات نهائياً، بما لا يدع مجالاً للإبقاء عليها بأي شكل من الأشكال، ومن ثم وقف أي شكوك تراود الفرد من أنه قد يضر أو يساء إليه من خلال تلك الملفات.

ومن هنا فإن الحق في المحو والإلغاء يعتبر أحد الضمانات الأساسية التي عمدت إلى ذكرها الاتفاقية الأوروبية لحماية المعلومات من أخطار بنوك المعلومات.

والخلاصة في رأينا أن الدول الصناعية والمتقدمة علمياً وتكنولوجياً قد أصدرت تشريعات خاصة بحماية البيانات والمعلومات في مواجهة أخطار التكنولوجيا الحديثة كالحاسب الآلي وبنوك المعلومات، ووضعت الضمانات اللازمة التي تعطي للفرد في السيطرة على معلوماته الخاصة التي تخزن في بنوك المعلومات وذلك للحد من الأخطار والاعتداءات التي يمكن أن تقع على هذه المعلومات إذا ما قام بحيازتها شخص آخر، والتي من شأنها أن تؤثر على حقوق وحرية الأفراد.

أما تشريعات الدول النامية ومنها التشريع الأردني فهي ما زالت في مرحلة النمو والتطور وانها لم تواكب التطور العلمي الحديث على كافة المستويات، كما هو موجود في الدول المتقدمة، لذلك وحسب إطلاعي ومعرفتي المتواضعة فإنه لا يوجد تشريع

(٣) المرجع نفسه، ص ١١٩.

خاص ومستقل في الأردن يعالج أو يتناول حماية البيانات من أخطار بنوك المعلومات، رغم التطور الهائل الذي حصل في الآونة الأخيرة.

بيد أن المشرع الأردني قد عمد إلى حماية بعض أسرار المهن، وبعض تشريعات البنوك وتوصف هذه الحماية بأنها حماية تقليدية (كحماية المذفات الطبية أو الأسرار المهنية بين المحامي والموكل، أو الأسرار التي تكون بين المصرف والعميل) وعلى الرغم من ذلك فإن هذه النصوص التقليدية لحماية شرف الإنسان وسمعته وحياته الخاصة لا تغطي إلا جانباً من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين المعلومات لدى هذه البنوك، ولذا فإن الفرد لا يستطيع الوصول إلى هذه المعلومات التي أخذت عنه لدى بعض المؤسسات الحكومية أو الخاصة والإطلاع عليها وتصويب ما هو خاطئ منها.

ولكن من خلال قراءة نصوص قانون الإحصاءات العامة، يُستشف من نص المادة (١١) والخاصة بسرية البيانات، أن المشرع أعطى الفرد ضمانات هامة وهي الحق في سرية جميع المعلومات والبيانات التي تؤخذ عنه، ولا يجوز استخدامها إلا في حدود الغرض الذي جمعت من أجله، كما أن المشرع أوجب على الدائرة اتخاذ كافة التدابير والإجراءات الكفيلة بحماية البيانات التي يتم جمعها وحفظها وأن تتحقق في تلك الأماكن شروط الأمان والسلامة، كما ألزم الموظف الذي يقوم بجمع البيانات بعدم إفشاء أو نشر أي معلومات أو بيانات إفرادية.

ونختم هذه المبحث بترديد مقولة لـ (Epperson) حيث يقول: المبدأ هنا هو ((ليس مجرد أن يعرف الفرد أن هناك معلومات عنه أو الاستخدامات التي ستخضع لها تلك المعلومات)) إنما المبدأ هو ((إدارة عادلة لتلك الملفات أو المعلومات)) (١) .

---

Michael Epperson (( Transnational Contracts for Eguivalency of Data <sup>(١)</sup>  
Profecction ,

information Services Securing P . 161

))  
نقلاً عن /المقاطع ، مرجع سابق ، ص ١٢٠

## الخاتمة

وبعد أن انتهينا بحمد الله وتوفيقه من بحث موضوع الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات ، باعتباره مطلب عزيز لكل فرد وضرورة ملحة لكل إنسان لا غنى عنها ، فإنه ينبغي لنا أن ندقي نظرة شاملة على الجوانب المختلفة لهذه الدراسة، وما انتهينا إليه من نتائج وتوصيات أملتتها دراسة الجوانب المختلفة لهذا الموضوع ، والمشاكل التي ثارت حوله في ظل التطور العلمي والتكنولوجي ، خاصة بنوك المعلومات والتي لعبت دوراً كبيراً في تهديد خصوصيات الأفراد ، إذا ما تم جمع وتخزين هذه المعلومات لدى هذه البنوك ، وتم استخدامها بطرق غير مشروعة .

فعلى الرغم من الأثر الإيجابي الواضح لنظم المعلومات على تطور المجتمع وبناء الحضارة الإنسانية الحديثة ، إلا أن لهذه النظم اثر سلبي وخطير على الأفراد وعلى التنظيم السياسي للدولة ، فقد مكنت التكنولوجيا الحديثة للمعلومات من المساهمة في تقييد الحقوق والحريات الشخصية للأفراد عن طريق جمع وترتيب وتخزين ومعالجة المعلومات الاسمية المتعلقة بهم في الحاسب الآلي كبنوك للمعلومات مما يهدد خصوصية حياتهم الخاصة والسرية اللازمة لها ويثير مخاوف على قدر كبير من الجدية .

ففي الحقيقة أن المجتمع الحديث أصبح يعتمد على المعلومات باعتبارها عصب الحياة الاقتصادية والسياسية والإجتماعية والعملية ، وأصبح الحاسوب من سمات بل وضرورات حسن التنظيم الإداري سواء على مستوى روابط القانون العام أم روابط القانون الخاص . ولقد وصف هذا العصر بأنه عصر الحاسوب وتكنولوجيا المعلومات .

وقد عرضنا في الفصل الأول من هذه الدراسة لأثر خطورة بنوك المعلومات على حق الفرد في خصوصية معلوماته ، واتضح لنا أن المعلومات تمثل الجيل الجديد من الحقوق والحريات في المجتمعات الحديثة ، فالمعلومات تمثل قيمة وثروة وتستطيع أن تصل إلى حد أن تصبح سلطة ، ويمكن عن طريق حفظ وتخزين ومعالجة المعلومات الشخصية لدى هذه البنوك المساس بحقوق وحريات الأفراد .

ولذلك اتخذت العديد من الدول المتقدمة مثل الولايات المتحدة الأمريكية ودول أوروبا الغربية الاحتياطات اللازمة لمواجهة التطور التكنولوجي لعصر المعلومات ، وتم إصدار العديد من التشريعات والاتفاقات الدولية لمواجهة هذا التطور ، وذلك من اجل حماية الأفراد في خصوصية معلوماتهم ، وفي نفس الوقت تفتح المجال لحصولهم على المعلومات .

وفي إطار هذا الفصل تناولنا بالدراسة ماهية الأشخاص الذين يمكنهم الاعتداء على حق الفرد في خصوصية معلوماته ، حيث تبين لنا أن الاعتداء قد يقع من الدولة أو من الهيئات العامة فيها باعتبارها صاحبة الولاية العامة على الأفراد ، ولاعتبارات المصلحة العامة تقوم بإنشاء بعض البنوك والتي تتضمن معلومات وبيانات عن الأفراد ، خاصة وان بعض هذه المعلومات تكون ذات طابع سري للغاية ، الأمر الذي يتوجب على هذه الهيئات أن تستخدم البيانات التي جمعت لديها في إطارها الصحيح وان تستخدم في الغرض المحدد الذي جمعت من اجله ، إذ انه في حالة إساءة استخدام مثل هذه المعلومات ، فإن الفرد قد يضر منها مما يترتب عليه انتهاك لخصوصية معلوماته وتهديد مصالحه المختلفة . وكذلك بالنسبة للهيئات والمؤسسات الخاصة فإن تأثيرها على حقوق وحرريات الأفراد لا يقل أهمية من التأثير الذي يتم عن طريق الهيئات العامة .

فمن طريق الربط بين الحاسبات الآلية وبنوك المعلومات التابعة لجهة الإدارة يمكن تجميع كافة المعلومات المتعلقة بالحياة الخاصة للفرد من كافة النواحي الشخصية والصحية والعائلية والمالية . كما يمكن استخدام هذا الكم الضخم من المعلومات بمعرفة سلطات الضبط الادراي للتأثير على الأشخاص وكوسيلة للضغط وفرض النفوذ ، ويمكن من خلاله الاعتداء على الحقوق والحرريات الشخصية وحرمة الحياة الخاصة ، بل والتأثير بطريق غير مباشر على كافة الحقوق والحرريات العامة للأفراد ، سواء الفكرية أو الاقتصادية أو الاجتماعية .

وفي المبحث الثاني من هذا الفصل عرضنا فيه بالدراسة لطرق الاعتداء على المعلومات الشخصية للأفراد ، ومن هذه الطرق التي تم معالجتها استخدام المعلومات المجمعة عن الفرد لغير الغرض الذي جمعت من اجله ، والتداول غير المرخص به للمعلومات ، والإفشاء غير المشروع للبيانات ، والأخطاء في المعلومات والبيانات ،

وذلك في أربعة مطالب مستقلة . ثم بينا موقف التشريعات المختلفة من هذه الطرق والتي تمثل تهديداً حقيقياً لخصوصية الفرد في معلوماته الشخصية ، حيث تم دراسة التشريع الفرنسي والأمريكي باعتبارهما نموذجين لنظامين قانونيين مختلفين ، هما النظام الانجلو سكسوني ويمثله التشريع الأمريكي ، والنظام اللاتيني ويمثله التشريع الفرنسي ثم عرضنا لموقف تشريعنا الأردني .

وتبين من خلال الدراسة المقارنة ان التشريع الفرنسي يعتبر من التشريعات المتقدمة في هذا المجال ، حيث تبين من خلال قانون العقوبات الفرنسي ، الصادر لعام ١٩٩٤ ، انه قد أضفى حمايته لمعالجة البيانات الاسمية في مواجهة بنوك المعلومات ، ونص على بعض الجرائم المتعلقة بالمعلوماتية ، كجريمة الانحراف عن الغرض أو الغاية من المعالجة الالكترونية وجريمة الإفشاء غير المشروع للبيانات الاسمية وجريمة التداول غير المرخص به للمعلومات وغيرها .

ولاندى في هذا المجال دور الفقه ، إذ كان للفقه الفرنسي الريادة في لفت الأنظار حول أخطار بنوك المعلومات على الحياة الخاصة بشكل عام ، وعلى المعلومات الشخصية للأفراد بشكل خاص ، ومدى تهديدها لها ، لما تملكه من قدرات فائقة في تخزين واسترجاع قدر كبير من البيانات في وقت قصير عن مختلف أوجه الحياة سواء عن الأفراد أو الجماعات، واثّر ذلك في اختلال التوازن بين السلطات السياسية في الدولة وبين الحاكم وأفراد الشعب .

ثم بحثنا موقف القانون الأمريكي من أخطار بنوك المعلومات على خصوصية الأفراد ، حيث تبين بان الفقه الأمريكي قد أدرك خطورة هذه الأنظمة على الحياة الخاصة للأفراد ، وطالب السلطات التشريعية بضرورة وضع الضمانات القانونية الكافية لحماية الأفراد وخصوصياتهم من خطر إساءة استخدام بنوك المعلومات .

ومن الجدير بالذكر أن المشرع الأمريكي لم يضع تنظيماً تشريعياً خاصاً لحماية المعلومات الشخصية للأفراد من أخطار بنوك المعلومات ، إلا انه نظم ذلك من خلال قوانين أخرى سواء الخاصة بحماية الخصوصية أو حماية البيانات الخاصة .

ثم عرضنا لموقف تشريعنا الوطني من هذه الأخطار التي تهدد خصوصية الأفراد في معلوماتهم الشخصية ، وباستقراء نصوص الدستور والتشريعات الجزائية الخاصة بحماية الحياة الخاصة أو التشريعات الخاصة بحماية البيانات لم نجد من بينها ما يكفل

هذه الحماية في مواجهة استخدام الحاسبات الالكترونية كبنوك للمعلومات ، وبحثنا مدى صلاحية المادة (٣٥٥) من قانون العقوبات الخاصة بحماية سر المهنة ، والمادة (١١) من قانون الإحصاءات العامة المؤقت رقم (٨) لسنة ٢٠٠٣ .

وخلصنا إلى أن المادة (٣٥٥) لا تحوي في ألفاظها أو مضمونها ما يحمل على إمكانية تطبيقها في حالة إفشاء المعلومات المخزنة في بنوك المعلومات ، وكذلك بالنسبة للمادة (١١) الخاصة بحماية سرية البيانات ، ولما كان القياس محظوراً في تفسير نصوص التجريم والعقاب فمن ثم فإن هذه النصوص لا تكفل حماية البيانات الشخصية في مواجهة أخطار بنوك المعلومات.

وهذا يعتبر قصور في تشريعنا الوطني مقارنة بالتشريعات في الدول المتقدمة.

والخلاصة في رأينا إلى أن هناك تبايناً في مواقف الأنظمة القانونية المختلفة بشأن مخاطر بنوك المعلومات على حق الفرد في خصوصية معلوماته ، فمنها من نصت دساتيرها على حماية الفرد في خصوصية معلوماته ، ومن هذه الدول اسبانيا ، البرتغال ، النمسا ، ومنها من نصت على ذلك في تشريعاتها العادية ، مثل فرنسا والولايات المتحدة الأمريكية ، النمسا ، بلجيكا ، ألمانيا ، النرويج ، ومنها من التزمت الصمت نحو هذه الأخطار وهي الدول النامية والتي اكتفت تشريعاتها بالنصوص الخاصة بحماية الأسرار ، ومنها تشريعنا الأردني .

وأخيراً تناولنا في الفصل الثاني من هذه الدراسة، مبادئ حماية المعلومات الشخصية وضماداتها في مجال تجميعها في بنوك المعلومات. حيث تكلمنا في المبحث الأول عن مبادئ حماية المعلومات الشخصية في بنوك المعلومات ، ونتيجة لتظافر جهود الفقه والقضاء والقانون المقارن فقد تم الاتفاق على وضع مجموعة من المبادئ والوسائل ، والتي تهدف إلى وضع الفرد في موقع متقدم في مواجهة تلك الاعتداءات ، كي يتمكن من السيطرة على معلوماته المخزنة عنه آلياً في بنوك المعلومات .

وقد لاحظنا من خلال تشريعات الدول المتقدمة علمياً وتكنولوجياً أنها عمدت إلى حماية المعطيات والبيانات الشخصية من خلال إقرارها لمجموعة من المبادئ والتي يمكن من خلالها التقليل من الآثار المحتملة التي تصيب الفرد في خصوصية معلوماته ، ومن هذه المبادئ على سبيل المثال مبدأ الأخطار العام ، مبدأ الأمن ، مبدأ الحماية المهنية ، مبدأ الشرعية وغيرها ، وقد تم تناول هذه المبادئ بالدراسة ، من خلال

تشريعات الدول من أمثال أمريكا ، فرنسا ، ألمانيا ، وموقف هذه التشريعات منها ، وتبين بأن معظم الدول قد كرست هذه المبادئ في تشريعاتها الوطنية .

فعلى سبيل المثال نجد أن جمهورية ألمانيا قد أكدت على مبدأ الأمن من خلال قانون ولاية هيسن لحماية البيانات والذي يهدف إلى منع إساءة استخدام المعلومات المجمعة إلكترونياً في بنوك المعلومات .

كما نلاحظ أن هذا القانون قد اخذ مبدأ الإخطار العام ، حيث ينبغي إخطار الشخص عند اختزان معلومات شخصية عنه لأول مرة ما لم يعلم باختزان تلك المعلومات بطريقة أخرى .

وفي تشريعنا الوطني فقد تبين لنا من خلال الدراسة ، انه اخذ بهذه المبادئ بطريقة غير مباشرة ، وقد استشف ذلك من خلال نص المادة ( ١١ ) من قانون الإحصاءات العامة والمتعلقة بسرية البيانات التي تؤخذ عن الفرد ، حيث تبين انه قد أخذ بمبدأ الشرعية ومبدأ الأمن ، ومبدأ الحماية المهنية .

أما المبحث الثاني من هذا الفصل فقد تناولنا بالدراسة لأهم الضمانات المتاحة للفرد في السيطرة على معلوماته الشخصية ، ورأينا أن غالبية التشريعات في الدول المتقدمة من أمثال أمريكا ، فرنسا وبريطانيا وألمانيا ، قد أعطت الفرد مجموعة من الضمانات منها حق الفرد الذي سجلت عنه المعلومات بالاطلاع ، الحق في الوصول إلى هذه المعلومات وتصحيحها ، والحق في المحافظة على خصوصية المعلومات وسريتها والحق في تأقيت المعلومات، وقد بينا من خلال الدراسة موقف التشريعات المختلفة من هذه الضمانات ، ففي أمريكا مثلاً اصدر الكونجرس عام ١٩٧٤ قانون الخصوصية لحماية المعلومات الشخصية المجمعة إلكترونياً ، وذلك بهدف حماية هذه المعلومات وصيانتها من عبث السجلات الفيدرالية ، كما نص هذا القانون على مجموعة من الضمانات التي تعطى للفرد من اجل السيطرة على معلوماته الشخصية ، وان تكون المعلومات في مأمن من وصول غير المرخص لهم .

كما يلاحظ أن المشرع الأردني قد اخذ بضمانة الحق في المحافظة على خصوصية المعلومات وسريتها وذلك من خلال القوانين الخاصة بحماية البيانات، ونشير هنا إلى قانون الأحوال المدنية الأردني ، وقانون الإحصاءات العامة .

ويتضح لنا في ختام هذه الدراسة أن هناك خطورة كبيرة على خصوصية الفرد في معلوماته الشخصية نتيجة للتوسع والتطور السريع في نظم المعلومات التي تعتمد على الحاسبات الآلية كبنوك للمعلومات ، وفي نفس الوقت فإن جمع المعلومات وتخزينها يعتبر من الاحتياجات الضرورية للمجتمع الحديث .



## نتائج الدراسة

هذا ، وبعد أن انتهينا من عرض النقاط الأساسية التي تضمنها البحث والقينا نظرة شاملة على أهم جوانب الدراسة ، يمكننا أن نجمل النتائج التي توصلنا إليها من هذا البحث في النقاط التالية :-

أولاً : أن المعلومات الشخصية للأفراد تمثل الجيل الجديد في عصر تكنولوجيا المعلومات ، فهي تمثل قيمة وثروة وتستطيع أن تصل إلى حد أن تصبح سلطة ، ويمكن عن طريق حفظ وتخزين ومعالجة المعلومات الاسمية في الحاسب المساس بحقوق وحرريات الأفراد والتأثير على حياتهم المستقبلية .

ثانياً :- أن بنوك المعلومات تمثل خطراً داهماً على حقوق وحرريات الأفراد ، خاصة حق الفرد في خصوصية معلوماته الشخصية ، إذا ما تم تجميع وتخزين هذه المعلومات واستخدمت في غير الغرض المعدة من اجله .

ثالثاً :- تعتبر الدول الصناعية المتقدمة علمياً وتكنولوجياً من أمثال أمريكا ، فرنسا ، ألمانيا وغيرها ، من الدول التي تنبعت إلى خطورة التكنولوجيا الحديثة المتمثلة ببنوك المعلومات على المعلومات الشخصية للأفراد ، ويعود لها فضل السبق في إصدار التشريعات الخاصة بحماية البيانات من عبث المتطفلين على حياة وخصوصية الآخرين .

رابعاً : - أنه نتيجة لتظافر جهود الفقه والقضاء والقانون المقارن ، فقد تم الاتفاق على وضع مجموعة من المبادئ والتي تهدف إلى وضع الفرد في موقع متقدم في مواجهة تلك الاعتداءات ، لكي يتمكن من السيطرة على معلوماته باعتبار أن الخصوصية التي تدور حولها الحماية هي خصوصية المعلومات ، كما أن من شأن هذه المبادئ أن تقلل من مخاطر الاعتداء على المعلومات أو البيانات الخاصة بالأفراد ، إذا ما تم الأخذ بها والعمل على إبرازها في التشريعات العادية .

خامساً : - أن هناك دولاً التزمت الصمت في مواجهة أخطار بنوك المعلومات ، وهي غالبية الدول النامية ، ومنها التشريع الأردني ، حيث اكتفى بالنصوص الخاصة بحماية الأسرار ، وهذا يعتبر قصوراً في التشريع ، حيث انه لم يواكب التشريعات في

الدول المتقدمة والتي تنبعت إلى مخاطر بنوك المعلومات على حق الفرد في خصوصية معلوماته .

سادساً :- كان للتجربة التشريعية في بلدان مثل فرنسا دوراً بارزاً في حماية المعلومات الشخصية من مخاطر التكنولوجيا الحديثة ، وتلمسنا ذلك من خلال قانون العقوبات لعام ١٩٩٤ والذي جرم بعض الأفعال التي من شأنها ان تؤثر على حقوق وحرية الافراد ومنها جريمة المعالجة الالكترونية للبيانات دون ترخيص وجريمة الإفشاء غير المشروع للبيانات وغيرها ، وهذا يعتبر تطوراً جديداً في قانون العقوبات الفرنسي ، ناهيك عن اصدار بعض التشريعات الخاصة بالمعالجة الالكترونية للبيانات .

سابعاً :- عدم كفاية القواعد العامة التي تحمي سر المهنة لحماية الشخص في مواجهة أخطار بنوك المعلومات ، فإذا كان القانون يعاقب على إفشاء سر المهنة إلا إن هذه الأحكام تظهر عدم فاعليتها في الحماية إذا ما عرفنا إن السر يعرفه عدد كبير جداً من الموظفين والدعالمين في مجال الحاسب الآلي ، كما ان أعمال عقوبة إفشاء سر المهنة قد تقابله صعوبات ترجع إلى مبدأ التفسير الضيق في قانون العقوبات . لذا فان النصوص العقابية الخاصة بجريمة إفشاء الأسرار لا تصلح لحماية البيانات الاسمية التي تكون محلاً للمعالجة الآلية .

## التوصيات

لقد أصبح التوصل إلى البيانات والمعلومات عن الأشخاص أكثر يسراً وسهولة من ذي قبل بفضل استخدام الحاسب الآلي في النظام الموحد لبنوك المعلومات ، كما ازدادت الحاجة إلى السرية كي يتسنى حماية الأفراد والحفاظ على خصوصياتهم ، فالمعلومات التي كان من الصعب التوصل إليها نظراً لصعوبة الكشف عنها أصبحت سهلة المنال بتطبيق النظام الموحد للبنوك الذي ساعد على توافر وتكامل الحقائق عن الأفراد .

ومن بين النتائج المزعجة لسوء استعمال هذا النظام إمكان التعرف على الأفراد من خلال الحصول على المعلومات والبيانات التي تتصل بحياتهم الخاصة . لذلك يجب الحرص على ان لا يساء استعمال مثل هذه المعلومات اذا ثبتت أهمية وضرورة بقاء بنوك المعلومات، كما ان إساءة استخدام المعلومات المجمعة في هذه البنوك قد تؤثر في الحقوق الشخصية بصفة عامة وتضع قيماً على المجتمع الديمقراطي .

من هنا . فقد حاولنا من خلال هذه الدراسة إرساء مجموعة من الاقتراحات والحلول التي من شأنها أن تشكل في مجملها ضوابطاً قانونية تساعد على الحد من مخاطر بنوك المعلومات على حق الفرد في خصوصية معلوماته ، وذلك من خلال الاهتمام بما توصلت إليه التشريعات المقارنة في الدول المتقدمة في مجال تكنولوجيا المعلومات .

وبناءً على ما تقدم فقد توصلت هذه الدراسة إلى عدة توصيات ، متمنياً على المشرع ان يأخذ بها ومنها :-

أولاً :- أن يبادر بوضع تشريع خاص لحماية البيانات والمعلومات الشخصية للأفراد من أخطار إساءة استخدام بنوك المعلومات ، وذلك بتنظيم إنشاء هذه البنوك ومن له الحق في إنشائها وقواعد استخدامها وتحديد أغراضها والمجالات التي تعمل فيها والبيانات الشخصية التي يسمح بجمعها ومعالجتها إلكترونياً وحفظها ببنوك المعلومات .

ثانياً :- أن يتدخل بصورة واضحة وصريحة لتجريم حالات جمع البيانات الشخصية دون سبب مشروع ، ووسائل جمعها بطرق غير مشروعة ، وإساءة استغلال البيانات أو المعلومات الشخصية في غير الغرض المخصص لها ، وإفشائها للغير أو سلطات الدولة ، مسترشداً في ذلك بتشريعات الدول المتقدمة في الأنظمة القانونية المعاصرة ، تأكيداً على احترام حق الحياة الخاصة للأفراد وحررياتهم .

ثالثاً :- إخضاع أجهزة تجميع المعلومات لنظام قانوني دقيق من الترخيص للمحافظة على سرية المعلومات المخزنة فيها ، وفرض عقوبات مشددة في حالة إفشاء هذه المعلومات .

رابعاً:- إنشاء لجنة متخصصة وفق احكام القانون ولتكن المركز الوطني لتكنولوجيا المعلومات ، الا ان المشرع في قانون ضمان حق الحصول على المعلومات وفي المادة (٣) منه وتحديداً في الفقرة (٢) قد نص على انشاء مجلس المعلومات ، حيث يتكون هذا المجلس من تسعة اعضاء من بينهم مفوض المعلومات وهم مدير عام دائرة المكتبة الوطنية .

ولكن هذا المجلس لم يكن من صلاحياته دراسة المخاطر والاعتداءات التي تقع من الجهات القائمة على بنوك المعلومات ، وكذلك لم يكن من صلاحياته المراقبة والمتابعة لحماية خصوصية الافراد ولم يكن ايضاً من صلاحياته اعلام الشخص بأن هناك معلومات مسجلة عنه لكي يتمكن الفرد من الاطلاع عليها وتصويب ما هو خاطيء منها .

## قائمة المصادر والمراجع

أولاً : المراجع العربية :-

أ. المراجع العامة :-

- ١- د. احمد عوض بلال ، محاضرات في النظرية العامة للجريمة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠١
- ٢- د. كامل السعيد ، شرح الاحكام العامة في قانون العقوبات ، الطبعة الاولى ، دار الثقافة ، عمان ، ٢٠٠٢ .
- ٣- د. مأمون سلامة ، قانون العقوبات ، القسم العام ، الطبعة الرابعة ، دار الفكر العربي ، القاهرة ، ١٩٨٤ .
- ٤- د. محمد صبحي نجم ، شرح قانون العقوبات ، القسم العام ، الطبعة الثانية ، دار الثقافة ، عمان ، ١٩٩١ .
- ٥- د. محمود نجيب حسني ، شرح قانون العقوبات ، القسم العام ، الطبعة الخامسة ، دار النهضة العربية ، ١٩٨٥ .

ب. المراجع المتخصصة:-

- ١- أسامة احمد المناعسة ، جرائم الحاسب الآلي والانترنت ، دراسة تحليلية مقارنة ، الطبعة الأولى ، دار وائل للنشر ، عمان ، ٢٠٠١ .
- ٢- اسامة عبدالله قايد :-
  - أ. الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٨٩ .
  - ب. المسؤولية الجنائية للطبيب عن إفشاء سر المهنة ، بدون طبعة ، دار النهضة العربية ، القاهرة ، ١٩٨٧ .

٣- د. جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الكتاب الأول ، ( الجرائم الناشئة عن استخدام الحاسب الآلي ) ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ١٩٩٢ .

٤- د. حسام الدين كامل الاهواني ، الحق في احترام الحياة الخاصة ، الحق في الخصوصية ، بدون طبعة ، دار النهضة العربية ، القاهرة ، ١٩٧٨ .

٥- د. سعيد عبد اللطيف حسن ، إثبات جرائم الكمبيوتر والجرائم المرتبطة عبر الانترنت ، ( الجرائم الواقعة في مجال تكنولوجيا المعلومات ) ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ١٩٩٩ .

٦- د. عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، نظام التجارة الالكترونية وحمايتها مدياً ، الكتاب الأول ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٢ .

٧- د. عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٩٥ .

٨- د. عمرو احمد حسبو ، حماية الحريات في مواجهة نظم المعلومات ، بدون طبعة ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ .

٩- محمد أمين الشوابكة ، جرائم الحاسوب والانترنت " الجريمة المعلوماتية " ، الطبعة الأولى ، دار الثقافة ، عمان ، ٢٠٠٤ .

١٠- د. محمد عبد المدسن المقاطع ، حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسوب الآلي ، مطبوعات جامعة الكويت ، ١٩٩٢ .

١١- د. مدحت رمضان :-

أ. الحماية الجنائية للتجارة الالكترونية ، دراسة مقارنة ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠١ .

ب. جرائم الاعتداء على الأشخاص عبر الانترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ .

١٢- د. ممدوح خذيل بحر ، حماية الحياة الخاصة في القانون الجنائي ، بدون طبعة، مكتبة دار الثقافة ، عمان ، ١٩٩٦ .

١٣- د. ممدوح محمد المسلمي ، مشكلات البيع الالكتروني عن طريق الانترنت ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، ٢٠٠٠ .

١٤- د. نعيم مغرب ، مخاطر المعلوماتية والانترنت ، (( المخاطر على الحياة الخاصة وحمايتها )) ، دراسة مقارنة ، بدون ناشر ، بيروت ، ١٩٩٨ .

١٥- د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، بدون طبعة مكتبة الآلات الحديثة ، أسبوط ، ١٩٩٢ .

### ج. الرسائل الجامعية:-

١- د. آدم عبد البديع آدم حسين ، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، دراسة مقارنة ، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق ، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٠ .

٢- طارق احمد فتحي سرور ، الحماية الجنائية لأسرار الأفراد في مواجهة النشر ، رسالة مقدمة لنيل درجة الماجستير في الحقوق ، كلية الحقوق ، جامعة القاهرة ، ١٩٩١ .

٣- د. مبدر سليمان الويس ، اثر التطور التكنولوجي على الحريات الشخصية في النظم السياسية - رسالة دكتوراة ، جامعة القاهرة ، ١٩٨٢ .

٤- د. محمد عبد العظيم محمد ، حرمة الحياة الخاصة في ظل التطور العلمي الحديث، رسالة مقدمة لنيل درجة الدكتوراة في الحقوق ، كلية الحقوق ، جامعة القاهرة، ١٩٨٨ .

٥- يونس عرب ، جرائم الحاسوب ، دراسة مقارنة ، رسالة مقدمة لنيل درجة الماجستير في الحقوق ، كلية الدراسات العليا ، الجامعة الأردنية ، عمان ، ١٩٩٤ .

#### د. الأبحاث العلمية :-

١- د. حسام الدين الاهواني ، حماية خصوصية المعلومات في مواجهة الحاسب الآلي، مع دراسة خاصة لقانون الأحوال المدنية رقم ١٤٧ لسنة ١٩٩٤ ، أبحاث ودراسات المؤتمر العلمي الثالث لنظم المعلومات وتكنولوجيا الحاسبات المنعقد في القاهرة في الفترة من ١٢ - ١٤ ديسمبر ١٩٩٥ .

٢- د. سامر الدالعة ، مشكلات الحق في الخصوصية في ظل الاستخدامات اللامنهجية لبنوك المعلومات ، دراسة مقارنة ، بحث مقدم للنشر في مجلة اليرموك ، جامعة اليرموك ، لسنة ٢٠٠٧

٣. عدلي حسين ، الحماية الجنائية الاجرائية لحرمة الحياة الخاصة ، بحث مقدم الى مؤتمر الحق في حرمة الحياة الخاصة المنعقد بكلية الحق ، جامعة الاسكندرية في الفترة من ٤ - ٦ لسنة ١٩٨٧

٤. كمال احمد الكركي ، النواحي الفنية لإساءة استخدام الكمبيوتر ، بحث مقدم إلى ندوة " الجرائم الناجمة عن التطور التقني " ، المنعقد في عمان في الفترة من ٢٨ - ٢٩ لسنة ١٩٩٨ .

٥- د. نائل عبد الرحمن صالح ، واقع جرائم الحاسوب في التشريع الجزائري الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت ، المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة ٢٠٠٠ ،

٦ - يونس عرب ، الخصوصية وامن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخليوي ، بحث مقدم إلى منتدى العمل الالكتروني ، اتحاد المصارف العربية ، المنعقدة في عمان في الفترة ما بين ٢٠ - ٢٢ أيار ٢٠٠١ .

#### هـ . الدوريات :-

١ - احمد فتحي سرور ، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد ، العدد الرابع والخمسون . لسنة ١٩٨٤ .



٢. د. حسام الدين الاهواني ، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الالكتروني ، مجلة العلوم القانونية والاقتصادية ، العددان الأول والثاني ، السنة الثانية والثلاثون ، لسنة ١٩٩٠ ،

٣. د. غنام محمد غنام ، الحماية الإدارية والجناحية للأفراد عند تجميع بياناتهم الشخصية في أجهزة الكمبيوتر ، مجلة الأمن والقانون ، العدد الثاني ، أكاديمية شرطة دبي ، السنة الحادية عشر ، يوليو ٢٠٠٣ .

٤. نعيم عطيه ، حق الأفراد في حياتهم الخاصة ، مجلة إدارة قضايا الحكومة ، العدد الرابع ، السنة الحادية والعشرون ، ١٩٧٧ .

ثانياً :- مواقع على شبكة الويب العالمية (الانترنت )

١. [http : // WWW . Privacy International . Org](http://WWW.PrivacyInternational.Org)
٢. [http : // www.FTC GOV / Reports / Privacy3. html](http://www.FTC GOV / Reports / Privacy3. html)
٣. [Law Offic @ not . com . jo](http://Law Offic @ not . com . jo)

ثالثاً :- القوانين والتشريعات :

- ١- قانون العقوبات الأردني رقم ١٦ لسنة ١٩٦٠ . وفقاً لآخر التعديلات .
- ٢- قانون الإحصاءات العامة الأردني المؤقت رقم ٨ سنة ٢٠٠٣ .
- ٣- قانون الأحوال المدنية الأردني وتعديلاته رقم ٩ لسنة ٢٠٠١ .
- ٤- قانون الاتصالات الأردني رقم (١٣) لسنة ١٩٩٥ وتعديلاته .
- ٥- قانون المعاملات الالكترونية الأردني المؤقت رقم ٥٨ لسنة ٢٠٠١ .
- ٦- قانون ضمان حق الحصول على المعلومات الاردني رقم (٤٧) لسنة ٢٠٠٧ .
- ٧- قانون الأحوال المدنية المصري رقم ١٤٧ لسنة ١٩٩٤ .
- ٨- قانون العقوبات الفرنسي لعام ١٩٩٤ .