

مقرر قانون الخصوصية وحماية البيانات

د. أسماء روعي

المشرفة على قسم ماجستير القانون الرقمي

Law 621

المحاضرة السادسة
ماهية البيانات الشخصية
وأثر التكنولوجيا على الخصوصية





مقدمة عامة
ربط المحاضرة السابقة
بالمحاضرة الحالية



مقدمة عامة
ربط المحاضرة السابقة
بالمحاضرة الحالية



مقدمة عامة ربط المحاضرة السابقة بالمحاضرة الحالية

محاوّر المحاضرة
المحور الأول
ما هية البيانات الشخصية
المحور الثاني
أثر التكنولوجيا على الخصوصية

أولاً: المفهوم القانوني للبيانات الشخصية:

المحور الأول
ماهية البيانات الشخصية

ثانياً: موقف التوجيهات الأوروبية من البيانات الشخصية:

- 1- البيانات أو المعلومات التي تحدد هوية الشخص.
- 2- الشخص المعنى بالأمر.
- 3- الشخص الطبيعي المحدد الهوية أو القابل للتحديد.
- 4- مفهوم معالجة البيانات الشخصية.
- 5- مفهوم بطاقة أو ملف البيانات الشخصية.



المحور الثاني أثر التكنولوجيا على الخصوصية

ثانيًا: أثر الإنترنت على الخصوصية:

- 1- الإنترنت تزيد كمية البيانات المجمعة والمعالجة والمنشأة.
- 2- أثر البريد الإلكتروني على خصوصية المعلومات.
 - أ- جريمة تهديد الغير عن طريق البريد الإلكتروني.
 - ب- جريمة انتهاك سرية رسائل البريد الإلكتروني.
 - ت- جريمة تضخيم البريد الإلكتروني.
 - ث- جرائم اصطناع البريد الإلكتروني.

أولًا: مدى خطورة الكمبيوتر على الخصوصية:

- 1- الحاسوب لا يمثل خطورة متميزة على الخصوصية.
- 2- الحاسوب يمثل خطرًا داهما على الخصوصية.





3. أدوات الارتباط بالشبكة ووسائل الاتصال اللاسلكي وخصوصية المعلومات.
4. الحماية الجنائية للهوية الرقمية.
5. وسائل الدفع وعلاقتها بالخصوصية.

وثمة خمسة مبادئ أساسية تحكم ما يمكن تسميته بالممارسات العادلة والمقبولة أو النزاهة في نطاق خصوصية المعلومات أو حماية المعلومات الشخصية بشبكة الإنترنت.

المحور الأول ما هية البيانات الشخصية



مما لاشك فيه، إن البيانات الشخصية قد لاحقت التطور الذي شهدته شبكة الإنترنت؛ فلم تعد تقتصر البيانات الشخصية على البيانات التقليدية كالاسم واللقب والعنوان البريدي بل اتسعت هذه البيانات وتنوعت لتشمل صورة الشخص وصوته؛ كما أنها تضمنت بعض البيانات المتعلقة بالشخص ذاته من حيث قدرته المالية وسلوكياته وعاداته وميوله وأذواقه؛ والأكثر من ذلك كله البيانات التي تتعلق بجسم الإنسان " البيانات البيومترية ".

المحور الأول ماهية البيانات الشخصية



أولاً: المفهوم القانوني للبيانات الشخصية.
ثانياً: موقف التوجيهات الأوروبية من البيانات الشخصية.

حيث عرف المشرع الفرنسي البيانات الشخصية في ضوء القانون رقم ٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية؛ حيث نصت المادة الثانية على إنه " يعتبر بياناً شخصياً أى معلومات تتعلق بشخص طبيعي معروف هويته أو يمكن التعرف على هويته سواء بشكل مباشر أو غير مباشر، أو يمكن تحديد هويته بالرجوع إلى الاسم ورقم تعريفه الشخصي وبيانات الموقع والمعرّف عبر الإنترنت لواحد أو أكثر من العناصر المحددة الخاصة بالهوية الشخصية أو الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية ".

فالبيانات تعتبر "شخصية" طالما أنها تتعلق بالأشخاص الطبيعيين الذين تم تحديد هويتهم بشكل مباشر أو غير مباشر؛ كما أنه يمكن التعرف على شخص وتحديد هويته عندما يظهر اسمه على سبيل المثال في ملف؛ فهذا الأخير قد يحتوى على معلومات تسمح بشكل غير مباشر بتحديد هويته مثل عنوان " IP " أو الاسم أو رقم التسجيل أو رقم الهاتف أو الصورة الفوتوغرافية أو البيانات البيومترية مثل بصمة الأصابع أو الحمض النووي وكذلك جميع المعلومات التي يكون من شأنها تمييز الأشخاص عن غيرهم مثل مكان الإقامة والمهنة، والنوع، والسن.

كما عرفتھا اللائحة 679 / 2016 على أنها " بيانات شخصية ناشئة عن معالجة تقنية أو فنية خاصة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية للشخص الطبيعي والتي تمكنا من تحديد هويته من خلال صورة الوجه أو البيانات الخاصة ببصمات الإصبع " .

ويلزم توافر مجموعة من الشروط حتى يمكن الاستعانة بهذه البيانات واستخدامها: فيجب أن تكون هذه البيانات فريدة ودائمة وقابلة للقياس؛ حيث يمكن من خلال الأجهزة التقنية الحديثة تحديد هوية الشخص من خلال الرجوع إلى خصائص أو صفات الجسم مثل بصمة الأصابع أو الخطوط العريضة لكف اليد، وتحليل الشبكية، وقزحية العين، والشبكة الوريدية للإصبع واليد أو شكل الوجه وكذلك الحمض النووي؛ فكل هذه البيانات البيومترية المستخرجة من هذه الخصائص أثناء التسجيل هي بيانات شخصية.

حيث تستطيع البيانات البيومترية أن تحدد بطريقة تكنولوجية وفنية هوية الشخص من خلال تحويل صفة أو سمة سلوكية لشخص معين إلى بصمة رقمية؛ حيث تهدف هذه البيانات إلى إثبات انفراد الشخص بمظاهر ثابتة وغير قابلة للتغيير على جسده.

ونص قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 في الفصل الأول الخاص بالتعريفات في المادة الأولى على تعريف البيانات الشخصية: أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى كالاسم أو الصوت أو الصورة، أو رقم تعريفى، أو محدد للهوية عبر الانترنت أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية.

التوجيه: هو تشريع وفق نظام القوانين في الاتحاد الأوروبي؛ والذي يلزم الدول الأعضاء في الاتحاد الأوروبي بتطبيقه من حيث المضمون ولكن من غير الإلزام بالكيفية، يختلف التوجيه في قوانين الاتحاد الأوروبي عن **التنظيم**، حيث أن الأخير يجب أن يدخل قانونًا في حيز التنفيذ في الدول الأعضاء.

عرف التوجيه الأوروبي البيانات الشخصية في الفقرة الأولى من نص المادة الثانية بأنها " أي معلومات أو بيانات يكون من شأنها تحديد هويته شخص طبيعي محدد أو تكون قابله لتحديدته ".

كما أضاف التوجيه للتعريف المنصوص عليه في الفقرة الأولى من نص المادة الثانية " بأن الشخص يمكن تحديد هويته الشخصية بشكل مباشر أو غير مباشر ولا سيما من خلال الرجوع إلى رقم الهوية أو من خلال مجموعة من المعطيات أو الرموز المتعلقة بخصائصه الجسمية أو الفيزيولوجية أو الجينية أو النفسية أو الاجتماعية أو الاقتصادية أو الثقافية.

مع الوضع في الاعتبار، أن نص المادة الأولى من توجيهه EC / 48 / 46 و EC / 2002 / 58 تشير إلى أن الهدف الأساسي من هذه القواعد والنصوص هو حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين عند معالجة البيانات الشخصية و المتعلقة بحياتهم الخاصة.

وليس هناك أدنى شك ، في أن الدقة التي جاء بها تعريف البيانات الشخصية في نص أن الشخص يمكن تحديد هويته بشكل مباشر أو غير مباشر يؤكد على التوجيه من ضرورة تحقيق أعلى مستوى من الحماية للبيانات الشخصية داخل المجتمع، وبالتالي، لا تنطبق الحماية على المعلومات التي تحدد هوية الشخص بشكل مباشر مثل الاسم أو موطنه فحسب، ولكن أيضا على المعلومات التي تحدد العناصر التي تحدد شخصًا بشكل غير مباشر والتي ترتبط في الغالب بالتقنيات الحديثة: رقم الجوال أو عنوان البريد الإلكتروني أو رقم بطاقة ائتمان أو بيانات شخصية مثل صوته أو بصمات الأصابع، أو الحمض النووي أو حتى غيرها من البيانات البيومترية.

وسوف نتعرض إلى العناصر التي تضمنها التعريف الخاص بالبيانات الشخصية في التوجيه الأوروبي:



ثانيًا: موقف التوجيهات الأوروبية من البيانات الشخصية:

- 1- البيانات أو المعلومات التي تحدد هوية الشخص.
- 2- الشخص المعني بالأمر.
- 3- الشخص الطبيعي المحدد الهوية أو القابل للتحديد.
- 4- مفهوم معالجة البيانات الشخصية.
- 5- مفهوم بطاقة أو ملف البيانات الشخصية.

أن التعبير " أية بيانات أو معلومات " الوارد في نصوص التوجيه الأوروبي يدل على رغبة المشرع في الأخذ بمفهوم واسع للبيانات ذات الطابع الشخصي. حيث يتضمن مفهوم البيانات الشخصية جميع أنواع المعلومات المرتبطة بالشخص، مثل فصيلة الدم الخاصة بشخص معين. **وتندرج البيانات الأكثر خصوصية ضمن البيانات الشخصية** وفقًا لنص المادة ٨ من التوجيه بالنظر إلى المخاطر المحتملة الناشئة عن الاعتداء عليها.

ويقصد بالبيانات الأكثر خصوصية هي البيانات التي يدلي بها مستخدم شبكة الإنترنت عند دخوله موقع معين من أجل إتمام إجراءات الدخول على هذا الموقع؛ حيث يلزم على مستخدم الشبكة أن يسجل بعض المعلومات شديدة الحساسية مثل الميل الجنسي والآراء السياسية وديانته.

ومما لاشك فيه، أن مثل هذه المعلومات هي بيانات أكثر خصوصية تندرج ضمن قانون حماية البيانات الشخصية **التي يحظر معالجتها في حالات معينة؛ كما أنها تخضع إلى العديد من القيود.**

ووفقًا للتفسير الضيق، يشمل مصطلح " البيانات الشخصية " المعلومات المرتبطة بالحياة الخاصة والعائلية للشخص الطبيعي وكذلك المعلومات المرتبطة بأعماله أو أنشطته أيًا كانت مثل المعلومات المتعلقة بعلاقات العمل وكذلك المرتبطة بسلوكياته الاجتماعية، فالأمر يتعلق وفقًا للمفهوم الواسع أيضًا بالأشخاص الطبيعيين دون النظر إلى وظيفتهم أو صفاتهم مثل المستهلكين، والمرضى والموظفين، والعلماء، وما إلى ذلك.

فعلى سبيل المثال: يندرج ضمن البيانات الشخصية جميع المعلومات المرتبطة بوصفات العلاج التي يكتبها الطبيب من أجل شراء الدواء مثل رقم تعريف الدواء؛ وجرة الدواء؛ واسم الدواء؛ وسعر الدواء؛ وأسباب الاستخدام؛ اسم الطبيب، ورقم الهاتف؛ وما إلى ذلك، إما في شكل وصفات طبية فردية أو في شكل مجموعة من الوصفات الطبية، يمكن اعتبارها بيانات شخصية بالنسبة للطبيب الذي يقدم لمريضه الوصفة الطبية حتى ولو كانت البيانات الشخصية المتعلقة بالمريض تبقى مجهولة. **وبالتالي،** فإن تقديم المعلومات المتعلقة بالوصفات الطبية المكتوبة من قبل أطباء محددین أو هناك إمكانية أو قابلية لتحديدهم إلى الصيدليات ينطبق عليه مصطلح البيانات الشخصية الوارد في نص التوجيه.

ثانيًا: موقف التوجيهات الأوروبية من البيانات الشخصية:
1- البيانات أو المعلومات التي تحدد هوية الشخص:

هذا التفسير يتفق مع صياغة التوجيه نفسه؛ فمن ناحية أولى: يجب التأكيد على ما قضت به المحكمة الأوروبية لحقوق الإنسان من **اتساع مفهوم الخصوصية**. ومن ناحية أخرى، تتجاوز قواعد حماية البيانات الشخصية حماية المفهوم العام المتعلق بالحق في احترام الحياة الخاصة والعائلية.



ثانيًا: موقف التوجيهات الأوروبية من البيانات الشخصية:
2. الشخص المعني بالأمر:

هو كل شخص طبيعي تكون معطياته الشخصية موضوعًا للمعالجة؛ فعلى سبيل المثال، البيانات أو المعلومات المدرجة في الملف الشخصي للموظف بقسم شئون الموظفين؛ فهذه البيانات تعبر بصورة واضحة عن المعني بالأمر من حيث حالته الشخصية بصفته موظفًا، كما ينطبق ذلك أيضًا على النتائج الخاصة بالفحص الطبي للمريض في ملفه الطبي الموجود بالمستشفى أو صورة أو فيديو لشخص أثناء إجراء مقابلة معه.



ثانيًا: موقف التوجيهات الأوروبية من البيانات الشخصية:
3. الشخص الطبيعي المحدد الهوية أو القابل للتحديد:

يشترط التوجيه أن تكون المعلومات متعلقة بشخص طبيعي محدد أو قابل للتحديد؛ حيث يركز هذا العنصر على الاعتبارات الآتية:

بصفة عامة، يمكن اعتبار **الشخص الطبيعي محدد** عندما يكون "متميزًا" من بين جميع الأشخاص الآخرين داخل مجموعة من الأشخاص؛ بينما **الشخص الطبيعي القابل للتحديد** -والذي لم يكن في الإمكان تحديده بعد ولكن قابل للتحديد.

ومن المتفق عليه؛ أنه يمكن تحديد الهوية عادة عن طريق معلومات خاصة محددة لها علاقة بالشخص المعني بالأمر؛ نذكر منها على سبيل المثال؛ بعض العلامات أو المظاهر الخارجية للشخص مثل طوله، ولونه، وشعره، وملابسه... إلخ. أو صفة من صفات الشخص التي لا تكون واضحة مثل المهنة والوظيفة.

يتميز مفهوم معالجة البيانات الشخصية بالاتساع؛ بهدف تحقيق الحماية الكافية والشاملة في الجماعة الأوروبية، وقد ورد تعريف معالجة البيانات الشخصية بموجب المادة ٢ (ب) من التوجيه بطريقة يمكن من خلالها الإشارة إلى أي عملية تتعلق بالبيانات الشخصية: " أي عملية أو مجموعة من العمليات المبرمة والتي تستخدم الوسائل الآلية لكي تطبقها على البيانات الشخصية مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو التعديل أو التصميم أو الاستخراج أو الاسترجاع أو الاستخدام أو الإحالة عن طريق الإرسال أو النشر أو أي شكل آخر من الأشكال المتاحة مثل التقريب أو الربط البيني، أو القفل أو المسح أو التدمير ".

ويقصد بالربط البيني: هو إقامة ترابط مع معطيات أو بيانات مدرجة في سجل أو سجلات يمسكها مسؤول أو مسؤولون آخرون.

ويقصد بإحالة البيانات: يقصد بها إعطاء المعطيات الشخصية أو تسليمها أو إبلاغها بأي شكل من الأشكال وبأي وسيلة من الوسائل إلى شخص أو عدة أشخاص باستثناء المعني بالأمر.

ثانيًا: موقف التوجيهات الأوروبية من البيانات الشخصية:
5. مفهوم بطاقة أو ملف البيانات الشخصية:

حيث أشاد البعض بالدور الذي لعبه التوجيه الأوروبي CE/46/95 في تعريفه لمفهوم البطاقات حتى لا يتم الخلط بينه وبين معالجة البيانات؛ فالتوجيه عرف البطاقة على النحو التالي:
" أي مجموعة منظمة من البيانات الشخصية يمكن الوصول إليها وفقًا لمعايير معينة، سواء كانت هذه البيانات مركزية أو غير مركزية أو سواء كانت موزعة وظيفيًا أو جغرافيا ."



المحور الثاني
أثر التكنولوجيا على الخصوصية

تمهيد وتقسيم:

الحقيقة إن استخدام وسائل التقنية العالية - الكمبيوتر والإنترنت - في ميدان جمع ومعالجة البيانات الشخصية من قبل الدولة أو القطاع الخاص، قد عمق التناقضات الحادة التي برزت منذ القدم بين حق الأفراد في الخصوصية، وموجبات الإطلاع على شئون الأفراد.

وتتمثل التناقضات بين حق الفرد في الخصوصية، وموجبات الإطلاع على شئون الأفراد، بمعالم أربعة رئيسية:

(1) التناقض بين حق الخصوصية **وحق الدولة في الإطلاع على شئون الأفراد**، والذي عمقه تزايد تدخل الدولة في شئون الأفراد، وليس المراد بهذا التدخل الإطلاع على معلومات معينة عن الأفراد، ولكن لتنظيم الحياة الاجتماعية على نحو أفضل كالاحتفاظ بسجلات الولادات والزواج، والوفيات والإحصاءات وغيرها، وقد تستخدم للأسف الدولة للمعلومات الشخصية الخاصة بالفرد لأغراض تتناقض مع صونها واحترامها.

(2) التناقض بين حق الفرد في الاحتفاظ بسريته ومصالحته في كشف حياته الخاصة ليتمتع بثمار هذا الكشف ورغم أن هذا التناقض للوهلة الأولى غير متحقق باعتبار أن الاحتفاظ بالسرية حق، والكشف الطوعي عن هذه السرية حق أيضا، إلا أن احتمال استغلال المعلومات المعطاة طوعاً لأغراض غير التي أعطيت لأجلها يمثل انتهاكاً لحرمة الفرد وسريته.

(3) التناقض بين الخصوصية والحق في جمع المعلومات لغايات البحث العلمي، أو حرية البحث العلمي.

(4) التناقض بين الخصوصية وبين حرية الصحافة وتبادل المعلومات (الحرية الإعلامية).

وهذه التناقضات - كما أسلفنا - برزت منذ القدم بين حق الفرد في حماية حياته وبياناته الخاصة وبين موجبات الاطلاع على شئون الفرد، بما فيها تلك التي تقع ضمن نطاق خصوصيته. وإذا كانت الجهود التنظيمية، والإدارية والتشريعية سعت إلى إقامة التوازن بين هذه الحقوق المتعارضة، فإن استخدام التكنولوجيا في ميدان جمع ومعالجة البيانات الشخصية، قد خلق واقعا صعبا هدد هذا التوازن من جهة وعمق حدة التناقضات المشار إليها من جهة أخرى.

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 الحاسوب لجمع وتخزين، ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية، وسوف نوضح ذلك من خلال بيان مدى خطورة الكمبيوتر، و الإنترنت وبنوك المعلومات على الخصوصية، وذلك على النحو التالي:

أولاً: مدى خطورة الكمبيوتر على الخصوصية:

(ب) الحاسوب يمثل
خطراً داهماً على
الخصوصية.

(أ) الحاسوب لا يمثل
خطورة متميزة على
الخصوصية.



يري هذا الجانب من الفقه بأن الحاسوب لا يشكل أي خطورة تستأهل وجود قواعد قانونية خاصة، والحجج التي ساقها هذا الجانب من الفقه لتؤكد ذلك هي:

1- الحاسوب لا يستطيع أن يضيف لنا ما هو جديد في مجال الخصوصية، فمنذ أن وجد الإنسان في المجتمع وهناك الملفات، والبطاقات والمحفوظات (الأرشيف) تحتوي على معلومات خاصة، وتجميع هذه المعلومات في مجالات متعددة وقد تم ذلك قبل ظهور الحاسوب بفترة طويلة، إذن فهذه المعلومات والبيانات المأخوذة عن هؤلاء الأشخاص لا تشكل أي خطورة على حياتهم الخاصة ولم نسمع من قبل بمثل هذه الخطورة، وقد استخدمت جهات الإحصاء المختلفة البطاقات المثقوبة لتسجيل المعلومات قبل ظهور شرائط التسجيل الإلكتروني والأقراص الممغنطة، فكل ما هناك هو أن هذه الآلات الحديثة حلت محل الذاكرة في هذا الخصوص، وما هي إلا مرحلة تكنولوجية جديدة من مراحل تطور الحياة الاجتماعية، ذلك التطور الدائم الحتمي لذلك قيل بأن إدخال نظام الكمبيوتر واستخدامه في مجال جمع المعلومات والبيانات الشخصية ما هو إلا مرحلة تكنولوجية جديدة من مراحل تطور الحياة الاجتماعية الدائم و الحتمي.

2- يكفي لحماية الخصوصية في مواجهة الحاسوب أعمال القواعد القانونية التي وضعت من قبل وما استقر عليه القضاء بصفة عامة. فهناك الكثير من النصوص التي تتعلق بالقذف والنشر والمسئولية المدنية، وسر المهنة. فلا أن تخضع الملفات التي أعدت يدويا لقواعد تختلف ويجوز تطبيق تلك القواعد على تلك التي أعدت إلكترونيا. فالعملية أو الفكرة واحدة في الحالتين، وبالتالي لا معني لإنشاء قواعد قانونية جديدة لتنظيم استعمال الحاسوب.

3- إن صدور تنظيم تشريعي في مجال نظم المعلومات لا يخلو من ضرر، إذ إن القضاء قادر على أن يطوع النصوص والقواعد المتعلقة بحماية الأفراد حتى يجعلها صالحة لمواجهة كافة المخاطر التي يمكن أن يثيرها استخدام آلة الحاسوب.

4- إن الكمبيوتر يفضل نظم المعلومات اليدوية في مجال حماية الخصوصية؛ إذ يسهل إدخال نظام أمان إلى الحاسوب باعتباره مجرد آلة وبالتالي يمكن منع استخدام الحاسوب إلا لمن يعرف الرقم الكودي أي الشفرة اللازمة للدخول إلى المعلومات المخزنة به وبذلك فإن من يصل إلى الحاسوب لا يمكنه الإطلاع على هذه المعلومات بعكس الحال في الملفات اليدوية، كما أن الحاسوب وملحقاته توضع في مكان ظاهر وبالتالي يمكن توفير الضمانات اللازمة لحماية الخصوصية.

ويلاحظ على هذا الاتجاه أنه بالرغم من عدم اقتناعه وإعترافه بما ينطوي عليه استعمال الكمبيوتر من انتهاك لحرمة الخصوصية، إلا أنه لم يسلم باقتناعه وثقته في هذه الوسيلة حيث يحيطه بقدر من الحيطة والحذر.

ب. الحاسوب يمثل خطرًا داهمًا على الخصوصية:

أما الرأي السائد وأصبح صحيحا في الوقت الحالي - من وجهة نظرنا - وهو أن الحاسوب يمثل خطرًا داهما على الخصوصية، ومن ثم يجب وضع قواعد خاصة لحمايتها في مواجهة هذا الخطر، وحجج هذا الرأي تتمثل في الآتي:

1- نجد أن عملية جمع المعلومات تثير مشكلات معينة بالنسبة لخصوصيات الإنسان، كما تمثل بعض التهديدات لها أيضا، فإن ظهور أجهزة الكمبيوتر قد أدى إلى تضخيم بعض هذه المشكلات، ظهور مشكلات أخرى.

فقبل ظهور الكمبيوتر كانت المعلومات توضع في بطاقات، وكانت بالطبيعة محدودة العدد وموزعة في أماكن عدة، أما بعد ظهور الكمبيوتر فقد أمكن تجميع قدر هائل من المعلومات في حيز مكاني بسيط جدًا، كما تسمح باستعمالها في أقل وقت.

فهذا التغيير الهائل في الكم يصل بنا إلى التغيير في الكيف، حقا العناصر التي تتكون منها الأساليب الفنية للكمبيوتر ليست جديدة في ذاتها، ولكنها جديدة في أبعادها، فلا يمكن إهمال عامل التوسع الهائل في التجميع والاستعمال، فذلك يؤدي إلى خلق وضع جديد يحتاج إلى مواجهة جديدة في ذاتها وهذا التغيير الهائل في مجالي التجميع والترتيب:

ب. الحاسوب يمثل خطرًا داهيًا على الخصوصية:

أ- فمن حيث التجميع نجد أن الكمبيوتر يختزن فيه أكبر قدر ممكن من المعلومات في أقل فترة ممكنة وفي أضيق حيز ممكن، وتحفظ هذه المعلومات في ذاكرة الحاسوب بصفة دائمة، بحيث تمنع عامل الزمن من إدخالها في طي النسيان، ومن ثم لم يعد من الممكن الاعتماد على النسيان كستار لحماية الخصوصية.

ب- ومن ناحية الترتيب فإن القدرة الهائلة للكمبيوتر تمكنه من مزج المعلومات المختلفة المتعلقة بالشخص وتحليلها بحيث تعطي في النهاية صورة كاملة عن شخصيته وجوانبها المختلفة.

وجميع هذه المعلومات يمكن أن تهدد الخصوصية للإنسان، فيمكن تجميع كافة المعلومات المتعلقة بالخصوصية - حياته الصحية، والعائلية، والمالية - بحيث تصبح تحت تصرف من لا يريد الشخص اطلاعهم عليها.

ب. الحاسوب يمثل خطرًا داهمًا على الخصوصية:

ثانياً: نجد أن هناك مؤثرات معينة تؤثر في السياسة العامة للدولة منها: المركزية، والتركيز، والاحتكار واللوائح والسيطرة الفردية، وأن ذلك نتيجة طبيعية للنتائج الناجمة عن تشغيل أجهزة الكمبيوتر ذات القدرة على اختزان المعلومات واستعادتها فالمشاركة في المعلومات معناه المشاركة في السلطة، وأن احتكار المعلومات هو احتكار للسلطة وعليه فإن أجهزة الكمبيوتر أصبحت أداة من أدوات تركيز السلطة بحكم احتكارها للمعلومات، بل وصل الأمر إلى حد التنبؤ بأن أجهزة الكمبيوتر سوف تكون هي صانعة القرار.

وتتناسب الخطورة على الخصوصية، مع القدرة الفائقة لتخزين المعلومات في الكمبيوتر، وفي المقابل فإن اتباع سياسة تتسم بالحسم في جمع المعلومات، ربما يتعارض مع الديمقراطية فالمعلومات الأساسية يجب أن تكون تحت توجيه الجميع، ولا يسمح بقصرها على فئة قليلة أو مستبدة من المسؤولين.

وفي نفس الوقت يزداد الإشراف والسيطرة على الفرد من أجل التأكيد على أهداف اجتماعية وسياسية، وسرعان ما يصبح في الإمكان فرض الرقابة المستمرة على كل مواطن والحصول على ملفات كاملة مستوفاة عنه حتى اللحظة الأخيرة، تشمل أغلب المعلومات الشخصية عن الصحة، أو السلوك الشخصي للمواطن، بالإضافة إلى المعلومات المعتادة. وتصبح هذه المعلومات عرضة لأن تستعاد بياناتها فوراً عند الطلب، وبمجرد ما تحتاجها السلطة المختصة.

ب. الحاسوب يمثل خطرًا داهمًا على الخصوصية:

ثالثًا: إن استخدام أجهزة الكمبيوتر في حفظ السجلات قد وضع حدًا للقيود التي كانت مفروضة على حفظ السجلات بالطرق العادية.

رابعًا: وطبقًا لرأي آخر كانت حقوق الفرد - ومن أهمها حق الفرد في الخصوصية - فيما يتعلق بالمعلومات المعروفة عنه أفضل بكثير قبل عصر الكمبيوتر حيث:



أ- إن المعلومات التي كان يمكن الحصول عليها كان يحتفظ بها بصفة عامة على أساس من اللامركزية، بمعنى أنها كانت متناثرة ومبعثرة بين عدة جهات، فلم يكن من الميسور إتاحتها للآخرين. مما يؤدي إليه من ازدياد الحاجة إلى السرية كي يتسنى حماية الحياة الخاصة من خطر العلانية.

ب- إن المعلومات المتاحة كانت سطحية نسبيًا وذلك من حيث مضمونها، كما كانت هزيلة إلى درجة تفقدها جدواها، وغير مضمونة.

ت- إن غالبية الناس لم يكونوا على قدر من الكفاية لتأويل البيانات المتاحة واستخلاص النتائج منها.

ث. إنه لم يكن من السهل تعقب الناس في مجتمع متحرك باستمرار منها.

خامسا: إن تهديد حرمة الخصوصية قد يثور، إذا أفشيت المعلومات الشخصية بدون موافقة أصحابها، وذلك عند إدراجها في ذاكرة الكمبيوتر ثم الاطلاع عليها من قبل الغير فإن هذا الإفشاء بالطبع يؤثر على الخصوصية.

وذلك لأن زيادة تدفق المعلومات عن طريق الكمبيوتر تهدد قدرة الفرد على التحكم في تدفق المعلومات عن نفسه وبالتالي يكون حقه في الخصوصية في خطر، حيث تكون الحقائق المتعلقة بالخصوصية تحت رحمة رجل في مركز يسمح له أن يضغط على الأزرار فيجعل الآلة تستعيد المعلومات.

سادسا: يمكن للحاسوب عن طريق برنامج يختص بترجمة النبضات والارتجاجات الناتجة عن الأصوات التي تصطدم بالجدران الأسمنتية للحجرات ومعالجتها إلى كلمات وعبارات، وقد يؤدي ذلك إلى انتهاك الحق في الخصوصية.

ب. الحاسوب يمثل خطرًا داهيًا على الخصوصية:

سابعاً: كذلك تظهر خطورة الكمبيوتر عند حدوث أخطاء أو تغيير بالمعلومات الخاصة بالفرد، سواء عند تغذيته، بها، أو إعادة تنظيمها، أو تقويمها، ويمكن أن تكون هذه الأخطاء ناتجة عن عيوب ميكانيكية أو كهربائية، ومن صفات الكمبيوتر أنه من البساطة تغيير البيانات عند تغذيته دون أن يكتشف ذلك، وهو ما لا يحدث عند حدوث أي تغيير في السجلات العادية.

فوجود خطأ مثلاً عن الظروف المالية للشخص قد تؤدي إلى القضاء على المستقبل المالي للشخص؛ حيث توصل في وجهه أبواب المصارف، وهيئات الائتمان دون أن يدري غالباً لذلك من سبب فالسمعة التي اكتسبها الكمبيوتر من حيث قدرته على معرفة ما لا يعرفه أحد يجعل لأضعف الإشاعات إذا ما سجلت فيه صفة الحقيقة المطلقة.

ثامنا: ومن مخاطر الكمبيوتر على الخصوصية إذا كان لكل مواطن رقم قومي حيث تنص الثانية من القانون المصري رقم ٤٣ لسنة ١٩٩٤م، في شأن الأحوال المدنية على أن:
(تنشئ مصلحة الأحوال المدنية قاعدة قومية لبيانات المواطنين تشتمل على سجل خاص لكل مواطن يميزه رقم قومي منذ ميلاده وطوال حياته ولا يتكرر حتى بعد وفاته، وتلتزم جميع الجهات بالتعامل مع المواطن من خلال هذا الرقم).

ويؤخذ على الرقم القومي أن المواطن يحول إلى مجرد رقم في معاملاته مع جميع الجهات الحكومية، وغيرها مما يمس ذاتيته وهويته الإنسانية، وتتمثل خطورة الرقم القومي في تيسير الاطلاع على كافة المعلومات المخزنة على الكمبيوتر في الجهات المختلفة.

فمعرفة الرقم تسهل الاطلاع على المعلومات المتعلقة بالأحوال الشخصية من خلال المعلومات المخزنة على الكمبيوتر الخاص بمصلحة الأحوال المدنية، ويمكن كذلك الاطلاع على المعلومات المتعلقة بالحالة الصحية عن طريق المعلومات المخزنة في الكمبيوتر الخاص بجهة التأمين الصحي، ويمكن أيضاً الاطلاع على أسرار العمل بواسطة المعلومات التي يتضمنها الكمبيوتر الخاص بالتأمين الاجتماعي، كذلك بالنسبة للمسائل المالية لدى جهة الضرائب أو الملكية العقارية، فمن خلال الرقم القومي يمكن في لحظات الاطلاع على كم ضخم من المعلومات.

وهكذا **يختل التوازن القائم بين النظام والحرية وبين السلطة والفرد مما يعتبر مساسا بالحرية العامة والخصوصية.** وانعكاس ذلك على نشاط المؤسسات الديمقراطية وخاصة إذا كان محل هذه المعلومات، هو الآراء السياسية، أو الفلسفية أو المعتقدات الدينية، أو الانتماءات النقابية للأفراد أو الجماعات.

وخلاصة القول: إن الكمبيوتر بقدرته الهائلة في التعامل مع المعلومات سواء من التجميع أو المعالجة وصورته أمام العالم في عدم قدرته على الخطأ أو النسيان، قد جعل ذلك الخصوصية للفرد عالمًا شفافًا تظهر فيه أدق الأسرار المتعلقة بالحياة الشخصية، والعائلية، والمالية، والآراء والمعتقدات السياسية و الفلسفية.

ثانيا: أثر الإنترنت على الخصوصية:

قدم الإنترنت أداة أخرى للمجرمين، ويسر لهم الوصول للعديد من الأهداف علي النطاق العالمي، وإن وضع نظاما لحماية الخصوصية في بيئة الإنترنت عليه أن يراعي طبيعة التهديدات الخاصة التي تتعرض لها الخصوصية في نطاق استخدامه، فالإنترنت جعل فيه سلسلة من التحديات الجديدة في مواجهة خطط حماية الخصوصية وتتمثل هذه التحديات فيما يلي:

1. الإنترنت تزيد كمية البيانات المجمعة والمعالجة والمنشأة.

2. أثر البريد الإلكتروني على خصوصية المعلومات.

3. أدوات الارتباط بالشبكة ووسائل الاتصال اللاسلكي وخصوصية المعلومات.

4. الحماية الجنائية للهوية الرقمية.

5. وسائل الدفع وعلاقتها بالخصوصية وذلك على النحو التالي:



1- الإنترنت تزيد كمية البيانات المجمعة والمعالجة والمنشأة:

إن الإنترنت شهدت نماء التوجه نحو جمع البيانات المتوفرة في العالم الحقيقي، باعتبارها تصبح أكثر سهولة في بيئة الإنترنت من حيث قدرة الوصول إليها، وأكثر ملاءمة للتبويب بسبب تقنيات الحوسبة، وتصبح أسهل للتبادل في ضوء وسائل تبادل المعلومات بكل أشكالها التي اتاحتها الإنترنت وبرمجيات التصفح والتبادل والنقل فالبيئة التي تمر عبرها رحلة البيانات المتبادلة تغيرت بسبب الإنترنت، وترك الأفراد خلفهم الوسائل التقليدية في الوصول للمعلومات، وأصبح اعتمادهم أكثر فأكثر على الإنترنت؛ لأن الإنترنت مصدر غني بالمعلومات حول كل شيء، وفي نطاق مسائل الخصوصية تحديداً فإن المعلومات عن الأفراد، وعاداتهم، وهواياتهم ومسلكتياتهم وآرائهم، واتجاهاتهم قى التسوق أمست متوفرة في ظل الإنترنت.

وإن البيانات المنقولة والمتبادلة والتي يطلق عليها تعبيرات عديدة كنهر المعلومات المتدفق كناية عن دور الماوس من بين أدوات جهاز الكمبيوتر في عمليات تنزيل قدر كبير من المعلومات، قد تشمل عنوان بروتوكول الإنترنت لحواسيب الافراد، والمتصفح المستخدم، ونوع الحاسوب، وآخر ما قام به المستخدم في زيارته الأخيرة السابقة لزيارة الموقع، وربما المواقع الأخرى التي زارها ووقتها، وتاريخها، وبيان المعلومات التي أرسلت واستقبلت، وقد تتضمن أيضاً معلومات محرك البحث الذي استخدمه المستخدم للوصول الي الصفحه، وتبعاً لنوع المتصفح قد يظهر عنوان البريد الإلكتروني للمستخدم.

فهذه المعلومات التي قد تكون كافية للتعريف بالشخص، وأيضاً قد يتم اصطياها عن طريق تقنيات الكوكيز، وجمعها في نقاط عديدة في الرحلة عبر الشبكات، يمكن أن تتوفر لإعادة استخدامها، أو افشائها، أو تناقلها بين قطاعات معينة، وبعض المعلومات مهمة وضرورية لعمليات الشبكة والوصول لمواقع الإنترنت كرقم التليفون وعنوان بروتوكول الإنترنت الخاص، وبدونهما فالشبكة غير قادرة على العمل، ولكن هناك أجزاء من المعلومات قد لا تكون ضرورية لهذه العمليات وقد يكون جمعها لأغراض غير عمليات الشبكة، ومع المعلومات التي تجمع في مراحل شراء المنتجات أو لمجرد التسجيل أو الاشتراك بخدمات الموقع، فإن جمع هذه المعلومات قد يشكل بيانا بأنشطة الفرد، وفي مرحلة من المراحل تصبح هذه البيانات عند جمع شتاتها وتحليلها خاصة مع قيام برمجيات ذكية بذلك، مادة تكشف تفاصيل كثيرة قد لا يرغب الشخص كشفها وفي نفس الوقت تصبح هذه البيانات مادة غنية ومحللاً للبيع من جهة لأخرى لغايات الأعمال والأنشطة.

إن تقنيات مثل (الكوكيز) يجري تخزينها بمجرد زيارة الموقع على القرص الصلب لجهاز المستخدم، ويمكن الموقع من جمع المعلومات باستمرار عن المستخدم، والتي تتعلق باشتراكه على الخط، والمواقع التي زارها، وما يفضله ومقدار مكوثه في المواقع وغير ذلك. ففي بيئة الإنترنت تستخدم العديد من الوسائل التقنية لتتبع المعلومات الشخصية للمستخدمين، ومن أشهرها ما يعرف برسائل (كوكيز - cookie) التي تنتقل إلى نظام المستخدم بمجرد دخوله للموقع، وتتمكن من تسجيل بيانات تخص المستخدم، ومع أنها كوسيلة اتبعت ابتداء لغرض غير جرمي وهو إرسال بريد الكتروني من الشركات التجارية في إطار أنشطتها الدعائية إلا أن ذلك لا يمنع أنها تمثل كشفا عن بيانات قد لا يرغب الشخص في الكشف عنها، وهي في تطوراتها اللاحقة مثلت خير وسيلة لتتبع الأشخاص، وكشف حياتهم، بل وإهدار توقعهم في التخلي، واستخدمت لتمثل خير وسيلة لبناء دراسات التسويق وملاحقة الزبائن الى درجة أحدثت من حالات المضايقة مما أثار التساؤل حول مدى مشروعيتها ومدى مساسها بحرية الأفراد.

2. أثر البريد الإلكتروني على الخصوصية:

ويثور التساؤل أيضا حول البريد الإلكتروني، حيث يعد من الخدمات المهمة التي تقدمها شبكات المعلومات حتى إنه يمكن القول: إنه أصبح واحدًا من أكثر وسائل الاتصال شيوعًا.

وهو يسمح للأفراد بتبادل الرسائل بشكل فوري من خلال شبكات المعلومات إلا أنه نظرًا للصعوبة الكبيرة التي تعرض إيجاد رقابة تحكم عمل هذه الشبكات، فإنه لا يوجد ضوابط تحكم هذا البريد، مما أسفر عن ظهور بعض الاستخدامات غير المشروعة للبريد الإلكتروني والتي بدأت في الانتشار في الآونة الأخيرة.

ويشكل الاعتداء على البريد الإلكتروني العديد من الجرائم، وعلى سبيل المثال وليس الحصر، قد يتم استغلال البيانات الشخصية التي يتم كتابتها عند الاشتراك في خدمة البريد الإلكتروني من قبل الشركات التجارية و الأفراد في إرسال الرسائل التي تتضمن الدعاية والإعلان عن منتجاتهم، مثل الكحوليات، ونوادي القمار والألعاب العنيفة، وغيرها من المواد الضارة مما قد يسبب نوعا من الضيق للمستهدفين.

وقد تتخذ جرائم الاعتداء على البريد الإلكتروني صورة جريمة تهديد الغير (E-mail talking)، وقد تقع الجرائم على البريد الإلكتروني مثل جريمة تزوير البريد الإلكتروني (E-mail Spoofing)، وجريمة انتهاك سرية رسائل البريد الإلكتروني، وجريمة تضخيم البريد الإلكتروني (Spam). وسوف نعرض لأهم هذه الجرائم وذلك على النحو التالي:

أ- جريمة تهديد الغير عن طريق البريد الإلكتروني:

وذلك عن طريق إرسال رسائل عبر الشبكة إلى شخص أو عدة أشخاص **تنطوي على عبارات تسبب خوفا وترويعا له**. ولعل الشباب والأطفال أكثر الفئات التي يتم استهدافها لارتكاب مثل هذه الجرائم على سبيل المداعبة، أو كمحاولة لاستغلالهم في ارتكاب جرائم السرقة؛ حيث يؤدي ذلك إلى تعطيل الشبكة، وعدم إمكانية استقبال أية رسائل، فضلا عن إمكانية انقطاع الخدمة، وبالتالي تكبد خسائر مادية و معنوية غير محدودة.



مجرد الدخول إلى موقع البريد الإلكتروني والإطلاع على الرسائل الموجودة بداخله دون إذن من صاحبه، يعد جريمة انتهاك سرية المراسلات المكفولة بنصوص الدستور كما سبق وأن بينا. وتجرم المشرع الفرنسي فعل انتهاك حرمة المراسلات البريدية من قبل الفرد العادي، وأيضا من قبل الموظف العام.

أما بالنسبة للموظف العادي فذلك بمقتضى المادة (٢٦٦ - ١٥) عقوبات، والمعدلة بمقتضى الأمر رقم ٩١٦ - ٢٠٠٠ الصادر في ٢٢ سبتمبر ٢٠٠٠م، والتي دخلت حيز التنفيذ في ١ يناير ٢٠٠٢م، وتنص هذه المادة على أن (يعاقب بسنة حبس وغرامة ٤٥٠٠٠ يورو لكل من يقوم بسوء نية وبشكل احتيالي بفتح أو حذف أو تأخير أو تحويل المراسلات المسلمة وغير المسلمة إلى جهة معينة، وتحويلها إلى الغير، أو الإطلاع على محتواها، ويعاقب بالعقوبة ذاتها كل من يقوم بسوء نية باعتراض أو تحويل، أو استخدام، أو إفشاء المراسلات: المرسلة أو المحولة أو المستلمة بالبريد الإلكتروني، أو القيام بتركيب أجهزة معدة للقيام بتلك الاعتراضات).

وتنص هذه المادة على نوعين من حماية المراسلات وهما: المراسلات المكتوبة والمراسلات البعيدة أو المراسلات بطريق الاتصال عن بعد (المراسلات الإلكترونية).

ويجزم المشرع الفرنسي فعل انتهاك حرمة المراسلات البريدية الإلكترونية من الموظف العام بمقتضى المادة (٤٣٢ - ٩) عقوبات، والمعدلة بالقانون رقم (٦٦٩ - ٢٠٠٤م)؛ الصادر في 9 يوليو ٢٠٠٤م، المتعلق بالاتصالات الإلكترونية وخدمات الاتصال السمعي والبصري، وتنص هذه المادة على أن (يعاقب بالحبس مدة ثلاث سنوات وغرامة 45000 يورو كل من له سلطة عامة أو مكلف بمهمة عامة أثناء تنفيذه لوظائفه، أو بمناسبة تنفيذه لها، يأمر، أو يرتكب، أو يسهل تحويل، أو إلغاء، أو فتح المراسلات أو إفشاء محتواها خارج الحالات المنصوص عليها في القانون).

ويعاقب بالعقوبة ذاتها الشخص المذكور في الفقرة السابقة، أو الوكيل العامل بشبكات الاتصالات الإلكترونية المتاحة للجمهور، أو مزود خدمات الاتصالات عن بعد يأمر، أو يرتكب أو يسهل اعتراض المراسلات المرسلة أو المحولة أو المستلمة عبر الاتصالات عن بعد، أو استخدامهما، أو إفشاء محتواها أثناء القيام بوظائفه وخارج الحالات المنصوص عليها في القانون).

وينص قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 في المادة 18: جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة: يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 100 ألف جنيه أو بإحدى العقوبتين كل من أتلف أو عطل أو أبطأ أو اخترق بريداً إلكترونياً أو موقعاً أو حساباً خاصاً بأحد الناس، فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى هاتين العقوبتين.

وقد ترتكب هذه الجريمة من قبل الأفراد، أو الشركات، أو الحكومة، وعلى سبيل المثال ففي عام ٢٠٠٦م تقدمت الحكومة الأمريكية بطلب إلى شركة غوغل بتزويدها ببيانات العملاء لديها حتى وإن تطلب الأمر الكشف عن المراسلات البريدية، وذلك لزعمها بأنها تريد الكشف عن مخطط إرهابي.

وبالنظر للطبيعة القانونية للإتفاقية المبرمة للخصوصية المعلوماتية في أغلب الشركات في هذا الشأن مثل شركة غوغل- نجدها تضع بند الخصوصية في اتفاقياتها مع العملاء المستخدمين لهذه الخدمة المقدمة لهم من قبلها، وبالرغم من ذلك تجيز لنفسها بموجبه أن تراقب الاستخدام من قبل المستخدم الى أقصى حد يسمح به القانون؛ للاطلاع أو الكشف عن معلومات المستخدم الخاصة، وحسابه وبياناته ومحتوياته واتصالاته عند وجود لذلك سبب وبحسن من جانبها للاعتقاد بأنه من الضروري القيام بذلك، نية أو امتثالا للقانون، أو لأي إجراء قانوني متخذ ضدها، وكذلك لتتأكد وتتحقق من أي انتهاكات محتملة لهذا العقد، وبذلك تفرغ الخصوصية من محتواها ومن خصائصها، فأين هي الخصوصية إذا ؟ !

وتتم جريمة تضخيم البريد الإلكتروني عن طريق وصول عدد ضخم من رسائل مجهولة المصدر إلى حساب البريد الإلكتروني للمستلم النهائي، ويستخدم في إرسالها برامج معدة خصيصًا لذلك، وهي برامج محظورة لكونها تهدد قواعد البيانات بتضخيم قاعدة عمل البريد الإلكتروني؛ حيث يجد صاحب البريد الإلكتروني نفسه أمام سيل منهمر من الرسائل عديمة الفائدة، أو التي قد يصاحبها فيروسات، أو صور أو ملفات كبيرة الحجم، مما يترتب عليه ضياع وإهدار العديد من الملفات و الرسائل الهامة، أو إلغاء صندوق البريد علي أثر تضخمه وحمله فوق طاقة الاستخدام المقررة له، مما يسبب ذلك انتهاكًا للخصوصية، وقد يسبب خسائر اقتصادية ضخمة، خاصة بالنسبة للشركات والمؤسسات العامة في مجال التجارة الإلكترونية والتي تنتظر مئات الرسائل الإلكترونية يوميا بغرض إبرام الصفقات التجارية.

ونص قانون مكافحة جرائم تقنية المعلومات المصري المادة (25) رقم 175 لسنة 2018 على الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع:

يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الاسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع اليكترونى لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو أخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أم غير صحيحة.

ونص قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 في المادة (24) الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني. يعاقب بالحبس مدة لا تقل عن 3 أشهر وغرامة لا تقل عن 10 آلاف جنيه ولا تجاوز 30 ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريداً إلكترونياً أو موقعا أو حاسبا خاصا ونسبه زورا لشخص طبيعي^٤ أو اعتباري.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى من نسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة وغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة فتكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تزيد على 300 ألف جنيه.



يمكن أن تتخذ هجمات الاصطناع عدة أشكال، منها هجمات اصطناع البريد الإلكتروني الشائعة، وهجمات اصطناع مواقع الإنترنت، وهجمات انتحال هوية المتصل من خلال اصطناع حساب خاص الكتروني والذي غالبًا ما يُستخدم لارتكاب عمليات احتيال.

انضم إلى رأي الفقه القائل بأن المشرع المصري قد أسرف وتزايد في النص على هذه الجريمة، حيث كان من المتعين إدراجها ضمن الجريمة الواردة في نص المادة ١٨ من القانون والمتعلقة بالاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة، بحيث يضاف إلى فعل الاعتداء المجرم فعل الاصطناع، دون الحاجة للنص عليها استقلالاً والوقوع في هذا التزايد والاسترسال غير المبرر.

3- أدوات الارتباط بالشبكة ووسائل الاتصال اللاسلكي وخصوصية المعلومات:

قد يرى البعض أن وسائل الاتصال اللاسلكية تحديدًا مما يخرج عن نطاق الإنترنت، غير أن الإنترنت الآن أصبحت بيئة تكاملية مع مختلف وسائط التقنية العالية سواء في حقل الحوسبة أو الاتصال أو في نطاقهما المدمج معا ولا أدل على ذلك من حالة التكامل بين أجهزة الهاتف الخليوي وتقنيات تبادل واستعراض المعلومات، بل تمثل المساعدات الرقمية والمكاملات الرقمية وأجهزة كمبيوترات الجيب المرتبطة بالشبكة عبر تقنيات الاتصال عن بعد - الأقمار الصناعية - وشبكات وإدارات الهواتف الخلوية مثالا حيا لمدى التكامل والترابط بين بيئة الإنترنت - مخزن المعلومات الضخم - ووسائل الوصول إلى المعلومات.

وفي تطور يعكس خطراً غير مسبوق، شهدت تقنيات الاتصالات وتبادل المعلومات اللاسلكية توظيف وسائل وأدوات مراقبة وجمع معلومات وتنصت لا سابق لها، ففي سياق معالجة الاتصالات، فإن كثيراً من أنظمة الاتصال اللاسلكي تجمع المعلومات حول موقع الجهاز الخليوي، وموقع مستخدمه وإصدار أو تلقي المكالمات، والتقاط معلومات الموقع والاستخدام، ويمكن التقاطها حتى لو لم يكن الجهاز قيد الاستخدام، فمجرد أن يكون عاملاً دون إرسال أو استقبال يمكن التقاط هذه المعلومات والأخطر القدرة على نقل الحديث رغم عدم وجود الاتصال.



وقد أثار هذا الموضوع معركة شرسة في العديد من الدول في مقدمتها الولايات المتحدة نفسها، ومع ذلك فإن الحكومات والشركات معا توجهت لمثل هذه التقنيات، فالحكومات أرادت لها لتحكم الرقابة، وقطاعات الأعمال والشركات في القطاع الخاص - ونقص المهتمة منها بهذه التطورات لأعمالها - اهتمت بهذه التقنيات لما تتيحه المعلومات من فرص التسويق، ولتتيح لها أيضا- عبر استثمار مواقع الإنترنت التي ترتبط بخدمات لاسلكية من إرسال الرسائل التسويقية والربط التفاعلي مع مستخدمي الوسائل اللاسلكية، وتحديدًا الهواتف الخلوية.

تعد سرقة أو انتحال الهوية الرقمية من أحدث الجرائم وأكثرها انتشارًا، وهي جريمة يقوم بها الجناة بانتحال شخصية شخص معين، وذلك عن طريق الحصول على معلوماته الشخصية من غير علمه من أجل تحقيق غرض معين، فلكل مستخدم للإنترنت هوية في العالم الافتراضي، ولهذه الهوية حقوق وواجبات.

ولقد أصدر المشرع الفرنسي بناء على ما سبق القانون رقم ٢٦٧ لسنة ٢٠١١م الصادر في ١٤ مارس ٢٠١١، و أضاف المشرع بناء على ذلك المادة ٢٢٦ - ٤ - ١ في قانون العقوبات الفرنسي، وقد وردت المادة ضمن الجزء الخاص بالاعتداءات على الخصوصية في القانون الفرنسي، وتنص هذه المادة على أن: (يعاقب بالحبس سنة وغرامة ١٥ ألف يورو كل من يقوم بانتحال هوية الغير أو باستخدام واحدة أو أكثر من بيانات ذات طبيعة تسمح بتحديد هويته، وذلك بهدف إقلاق هدوئه أو هدوء الآخرين، أو بهدف المساس بشرفه أو اعتباره. ويعاقب علي هذه الجريمة بذات العقوبة عند ارتكابها من خلال شبكة الاتصالات المخصصة للعموم عن طريق خط الإنترنت).

ويرجع السبب في تدخل المشرع الفرنسي وإضافة المادة السابقة إلى أن الهوية الرقمية تحتوي على الكثير من البيانات الشخصية والسرية لصاحب الهوية أو المستخدم - مثل الاسم وعنوان المسكن، ورقم الهاتف، وعنوان البريد الإلكتروني - والتي تم انتهاكها على الإنترنت وخصوصا على مواقع التواصل الاجتماعي كالفيس بوك Facebook.



وفي الواقع، أنه من الصعوبة تحديد عناصر الهوية الحقيقية تحديدًا دقيقًا، ولكن يمكن تعريفها على النحو التالي: " هي كل ما يعبر عن الفرد في العالم الافتراضي بشكل يدل عليه هو فقط، ولا يدل على غيره في ذات الوقت، أو هي كل ما هو قطعي الدلالة على شخصية فرد بعينه في العالم الافتراضي ".

فالهوية الرقمية شكل معين من أشكال الهوية، وهي مجموعة البيانات الشخصية للفرد في العالم الافتراضي مع ملاحظة أن المشرع الفرنسي يعاقب على هذه الجريمة متى تم ارتكابها عن طريق الشبكات العامة المفتوحة للجمهور (الإنترنت)، أي أن المشرع لا يعاقب على الجريمة متى تم ارتكابها عن طريق شبكات الإنترنت الخاصة و المخصصة لجهات معينة.

5- وسائل الدفع وعلاقتها بالخصوصية:



في بيئة الإنترنت، فإن وسائل الدفع السائدة تتمثل بالبطاقات المالية، فتتطلب عمليات الشراء، وعمليات الإعلان، وطلب الخدمات، والمزادات في عالم الإنترنت تقديم اسم الشخص، ورقم هاتفه، وعنوانه، وبريده الإلكتروني وببساطة فإنها تتطلب معلومات تفصيلية تغيب فيها القدرة على التخفي خلافاً للعالم الواقعي.

ولهذا فإن حماية خصوصية التعاملات المالية في بيئة الإنترنت أحد أهم ضمانات وجود النشاط التجاري فيها وتطوره، فإن نظام الدفع المالي على الإنترنت بدون نظام حماية للخصوصية سينقلنا من عالم الدفع النقدي المستتر إلى عالم مليء بوسائل الكشف والتعريف تتزايد فيه قدرة تتبع الأشخاص ومشترياتهم.

وخلاصة القول: أصبح انتهاك حرمة بيانات الأفراد والمؤسسات المتصلة بشبكة الإنترنت - سواء بالسطو عليها أو التلاعب فيها أو تحريفها - من الأمور الشائعة، مما يؤدي إلى خسائر جسيمة لهذه المؤسسات أو لعملائها.



✓ وثمة خمسة مبادئ أساسية تحكم ما يمكن تسميته بالممارسات العادلة والمقبولة، أو النزاهة في نطاق خصوصية المعلومات، أو حماية المعلومات الشخصية بشبكة الإنترنت، وهذه المبادئ هي:-

1. الإبلاغ /
الإخطار:

ويراد بهذا المبدأ أن مستخدمي المواقع يتعين إبلاغهم من قبل مزود الخدمة أو الموقع ما اذا كان الموقع أو مقتضيات الخدمة ينطويان على جمع معلومات الشخصية، وإلى أي مدى تجمع هذه المعلومات أو تستخدم.

2- الاختيار
(Choice):

ويوجب هذا المبدأ التزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بشأن استخدام بياناته فيما يتجاوز غرض جمعها الابتدائي.

3- الوصول للبيانات
(Access):

ويوجب هذا المبدأ قدرة المستخدمين للوصول إلى بياناتهم والتثبت من صحتها وتحديثها.

4- الأمن
(Security):

ويتعلق هذا المبدأ بمسؤوليات جهات جمع البيانات المواقع ومزودي الخدمة بشأن معايير الأمن المتعين تطبيقها لضمان سرية المعلومات، وسلامة الاستخدام وحظر الوصول غير المصرح به لهذه المعلومات، وما تتضمن من وسائل كلمات السر والتشفير وغيرها.

5. تطبيق القانون
(Enforcement):

ويتعلق هذا المبدأ بالآليات المناسبة المتعين اعتمادها لفرض الجزاءات على الجهات غير المتوافقة مع المبادئ المتقدمة، وما يتصل بها من الممارسات غير النزيهة بشأن جمع المعلومات الشخصية في البيئة الرقمية.

وفي المقابل فإن هذه المبادئ الخمسة المقيدة لتعامل جهات المواقع مع المعلومات الشخصية، يتعين أن لا تنتقص من سمات مجتمع الإنترنت الديمقراطي، وهي في حقيقتها لا تتعارض مع هذه السمات؛ لأن موجبات ديمقراطية الإنترنت عدم التغول على حقوق المستخدمين، ولكن وحتى تكون عمليات الاستخدام في منأى من التشدد يعمل بالتوازي مع هذه المبادئ، مبدأ رضا وموافقة المستخدم إلى جانب الاستثناءات المقررة بموجب معايير تزويد الخدمة التي تتيح قدراً من الحرية لجهات جمع البيانات بموجب ما هو مقرر في نظم مسؤولياتها القانونية أو مدونات السلوك التي تحكمها. ومع ضوابط محددة لضمان صحة وسلامة الرضا وضبط الاستثناءات، أو ما يمكن تسميته الممارسات المسموح بها لجهات تزويد الخدمة وإدارة المواقع.

الخاتمة





كلية الحقوق
قسم القانون الجنائي

الحق في حرمة الحياة الخاصة
في مواجهة الجرائم المعلوماتية



رسالة مقدمة من الباحثة
أسماء حسن سيد محمد رويحي
للحصول على درجة الدكتوراه في الحقوق

لجنة المناقشة والعلم

الأستاذ الدكتور / مدحت عبد الحليم رمضان
أستاذ ورئيس قسم القانون الجنائي بالكلية

رئيسا ومناقشا

الأستاذ الوزير الدكتور / عمر محمد محمد سالم

أستاذ القانون الجنائي ووزير مجلسي الشعب والشورى

مشرفا وعضوا

المستشار الدكتور / عمر الشريف علي الشريف

مساعد وزير العدل لشئون التشريع

عضوا ومناقشا

٢٠١٣ - ١٤٣٤

• المراجع:

د. أسماء رويحي، الحق في حرمة الحياة
الخاصة في مواجهة الجرائم
المعلوماتية، رسالة دكتوراه، جامعة
القاهرة، سنة 2013.

• المراجع:

2. د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، مجلة الشريعة والقانون بطنطا، العدد الثالث والثلاثون، الجزء الثالث، ديسمبر 2018، والبحث منشور على الموقع التالي:

https://mksq.journals.ekb.eg/article_30623.html



تم بحمد الله الإنتهاء من شرح المحاضرة السادسة
مع تمنياتي بالتوفيق د. أسماء رويحي

روابط الصور المستخدمة في المحاضرة:

- 1) <http://www.soutalomma.com>
- 6) <https://images.app.goo.gl/ncHYtxV9KC4wrLs6A>
- (7-20) <https://images.app.goo.gl/qE9km6wFG8NtiAuj6>
- (8) <https://images.app.goo.gl/ReWK7sg8byHARfLs7>
- (9-37-42-44-46) <https://images.app.goo.gl/4T2Jy2anG1WRKDyj9>
- (10) <https://images.app.goo.gl/KAFf7RasjB4xph8a8>
- (14-16-17) <https://images.app.goo.gl/rwVAHXLxv9FEKBbG9>
- (23-33-47-48-50) <https://images.app.goo.gl/SKa6FnYa2ofExS8k8>



Thank You