

قضايا أخلاقية ومهنية واجتماعية

(5)

الخصوصية فى مجال السايبر

Privacy and cyberspace

يرجع الاهتمام بالخصوصية إلى ما قبل عهد السايبر .

ما المقصود بالخصوصية Privacy :

فى الماضى كان المقصود بها المعنى المادى المكانى [كالمنزل .. حجرتك الخاصة .. مفكرتك .. الخ] ولكن الآن صارت تشمل النفاذ (الوصول Access) والسيطرة control على المعلومات الشخصية . وعموماً القول أن الخصوصية تعنى حماية الشخص من التدخل والتأثير وإطلاع الآخرين على معلوماته [دون إذنه] . وتلبية رغبته بحفظ ما يريد حفظه دون الاعتداء عليه أو إفشائه . وقد أثرت التكنولوجيا على الخصوصية من حيث كمية المعلومات والسرعة ومدة حفظ المعلومات وأنواع المعلومات المتداولة كما يلى :

1. **الكمية amount** : كمية المعلومات الشخصية التى يمكن جمعها أصبحت هائلة ولا تحدها سعة مكانية.
 2. **السرعة speed**: التى يمكن بها ترسل المعلومات زادت زيادة كبيرة فلا نحتاج لزمن مؤثر لإرسال معلومات ضخمة من مكان بعيد لآخر .
 3. **المدة duration** : ويمكن حفظ المعلومات لمدى زمنى يقاس بالسنوات .
 4. **النوع kind** : يمكن تداول كل أنواع المعلومات الحرفية والعديدية والصور والأصوات ويمكن تداول كل أنواع المعلومات المالية بدقة وتوزيعها لكل أنحاء العالم .
- والتفرقة بين ما هو خصوصي وعام بعضها فطرى (طبيعى) natural لا يختلف الناس حوله وبعضها تمليه الأعراف normative .
- ولذلك فهناك اتفاق عالمي حول الخصوصية نابع من الجانب الفطرى (الطبيعى) وهناك اختلاف فى جوانب أخرى بسبب الأعراف والثقافات . (فمن الثقافات ما يقدم مصلحة الفرد على مصلحة المجتمع) .
- ويمكن تعريف الخصوصية على أنها تهيئة اجتماعية تمكن الأفراد مستوى من السيطرة فى تحديد من ينفذ (يصل) لهم ولمعلوماتهم .

كيف تؤثر تكنولوجيا السايبر على الخصوصية :

تهددها من ثلاثة مناحي:

1. جمع البيانات .
2. تبادل البيانات .
3. بحث / تنقيب البيانات Data Mining

1. جمع البيانات نقصد بها جمع وتدوين و تخزين المعلومات الشخصية (وفى معظم الأحيان) دون علم صاحبها .

والمعلومات قد تتكون من النص text والصوت Voice والصورة video ويتم جمعها عبر عدة وسائل منها الآلات التصوير (كاميرات) المتخذة للمراقبة Surveillance .. تُجمع البيانات عبر الانترنت وتُخزن وتُحلل

(للتعرف واكتشاف الأنماط .. وظاهرياً ليس من اجل التعرف على معلومات تخص فرداً بعينه وانما لمعرفة كم من الناس يفعلون كذا وكم منهم يرغب فى كذا .. الخ) ومنها تدوين وتحليل المعلومات الصوتية (المحادثات الهاتفية) وتدوين آلياً مما يجعل هذه العملية سهلة .

ومن أنواع التدوين والتخزين لاكتشاف الرغبات والانماط وسيلة الـ Internet cookies [كلمة cookie تعنى قطعة البسكويت أو الكعك الصغيرة التى يحتفظ بها قريباً ليتناولها المرء كلقمة خفيفة سريعة ورشيقة تذهب الجوع لحدٍ ما] فالـ Cookie عبارة عن ملف صغير تخزنه إحدى تطبيقات الـ www فتضع فيه معلومات تخص المستخدم ويخزن فى القرص الصلب الخاص بالمستخدم فى نظامه. و هي فى الغالب دون إذن المستخدم [أى أن الحالة العامة default هى وجود الـ Cookie وحين يؤخذ إذن المستخدم تأتيه الرسالة Disable Cookies? Yes/no - و معظم المستخدمين لا يهتمون بذلك] و هي عادةً مفيدة للتجارة الالكترونية فلو إنك استخدمت تطبيقاً للمرة الثانية فإنها تأخذك الى حيث وقفت فى المرة الأولى ... (جرب استخدام مكتبة Amazon.com) ورغم أنها تدخل واستغلال المجال المستخدم إلا أنها مفيدة لو وقفت عند هذا الحد.

وتتضاعف المشكلة لوجود شركات متخصصة فى هذا المجال . فتكون لشركة واحدة اكثر من cookie فى نظامك وبالتالي فليديها معلومات عن تصرفاتك . وظاهرياً تعامل كل واحدة على حده ولكن وجود المعلومات بهذه الصورة قد يعرض خصوصية المستخدم للاختراق .

الخلاصة: الـ cookies تتسبب فى مخالفتين :

1. وضع مادة فى حيز المستخدم دون إذنه أو علمه .
2. الاستفادة من بعض هذه المعلومات دون علمه أو اذنه (وفى حالة الاستفادة منها - بيعها لا يكون للمستخدم نصيب !) ولذلك فان الـ Cookies ربما تخرق خصوصية المستخدم.

2. تبادل المعلومات الشخصية: المعلومات التى تجمع كثيراً ما تباع (للأغراض التجارية مثلاً: تباع قوائم عناوين بريد الكترونى مثلاً لارسال الدعايات لهم . أو تباع قائمة بريد الكترونى للذين يدخلون مواقع المكتبات ويبحثون عن كتب حاسوب ليرسل لهم ناشروا الحاسوب دعاياتهم وهكذا) وهذه المعلومات

المتنوعة ترسل بإذن أهلها أو دون أذنهم غالباً فتباع مثلاً لمكاتب التسليف Credit Bureau أو تكون فيها معلومات صحية سرية فتباع لمكاتب الترخيم (لمعرفة الحالة الصحية الحقيقية المتقدم للوظيفة) .

3. **بحث بيانات شخصية واستخلاص نتائج منها Data Mining Personal Data** استخلاص نتائج لمساعدة متخذى القرار .

والنتائج قد تكون غير واضحة وربما غير متوقعة وذلك بالبحث فى البيانات لإيجاد أنماط ضمنية من مخزن معلومات كبير وربما ينتج عن ذلك ضم الشخص لمجموعات ليس له علاقة بها (مجموعة الذين نقل أعمارهم عن الخمسين وارصدتهم بالبنك تتعدى المائة مليون دينار ، ومجموعة الذين حصلوا على سلفيات وتعثروا فى سدادها .. الخ) . ويستخدم التنقيب فى الانترنت لمعرفة الاتجاهات لدواعى تجارية وينتج عنه تصرفات تخدم تلك الأهداف . [وقد تطرقنا فى المحاضرة إلى مثال : شخص رفض البنك منحه سلفية رغم أنه مستوف لجميع الشروط وذلك بسبب مطابقة مواصفاته كالعمر والدخل لفئة تقلس بعد عام من تأسيسها لشركات خاصة] . وهكذا فقد أصبح ذلك الشخص ينتمى لفئة ليس له بها علاقة ولا يعرفها وحكم عليه على اساس أنه فرد من افرادها وتضرر من ذلك .

اما المدافعون عن التنقيب فيردون أن الحقائق التى استخدمت ليس جزءاً مباشراً من المعلومات إنما هو جزء ضمنى

(غير صريح Implicit) وأن المعلومات لم تنقل من مؤسسة أخرى وانما هى معلومات المؤسسة المتراكمة . وعلى كل فإن القوانين (فى البلاد تثار فيها هذه القضايا) تبنى للتجريم على الاختراق الذى يحدث :

i . من معلومات صريحة .

ii . طبيعتها سرية .

iii . أو حدث تبادل من قاعدة معلومات لأخرى .

وهذه النقاط الثلاثة لا تنطبق على التنقيب ولذلك فإن الخصوصية لا تحميها قوانين ولا أعراف من الانتهاك من جراء التنقيب . والان يستخدم التنقيب فى الانترنت لمعرفة الاتجاهات لدواعى تجارية وتنتج عنها تصرفات وخطط لخدمة تلك الأهداف التجارية .

حماية الخصوصية الشخصية فى المعلومات المعلنه:

المعلومات الشخصية مثل اسم الشخص، المؤهلات.. الخ هى معلومات عامة متاحة للجمهور وتخزن فى مواقع متاحة للجمهور . وهنالك معلومات شخصية غير معلنه وليست للاعلان .

المعلومات الشخصية (المتاحة لجمهور) العامة (PPI) Public Personal Information .

المعلومات الشخصية (الغير متاحة لجمهور) الخاصة (NPI) Non-Public Personal Information .

وقد اهتمت القوانين بالنوع الثانى (NPI) ولكنها لم تهتم بالنوع الأول (PPI) على اعتبار أنها معلومات عامة (متاحة) .

فقد تؤخذ هذه المعلومات الشخصية المعلنة وتربط مع أخرى معلنة ولكنها تعطى معانى أو تصورات لا يوافق عليها صاحب المعلومات .

محركات البحث Internet Search Engines:

تجمع معلومات من عدة مواقع بعضها بعلم صاحبها وبعضها دون علمه. ويمكن تكوين ملامح عن الشخص وهواياته واهتماماته بسهولة (أكثر من الحصول عليها من ملفات مفرقة فى عدد من المؤسسات والبلدان). هل كون المعلومات متاحة وتسمح بتصفحها يبرر عدم حمايتها ؟ كثير من المعلومات تتيحها البلديات للبحث الفورى والاطلاع لاقسامها المختلفة لتسهيل العمل ولأنهم لا يتوقعون أنها ستسبب ضرراً. وحالياً هنالك شركات تجمع تلك المعلومات ويستخرج منها مؤشرات تباع للجهات المختصة . ولكن ايضاً فان إتاحة تلك المعلومات (مثلاً خُطَر المنازل المخزونه لدى البلدية) قد يضر بأصحابها ولذلك يجب وضع هذه الحقائق فى الاعتبار والنظر فى حماية المعلومات .

الوسائل المحسنة للخصوصية Privacy Enhancing Tools:

نظم وتطبيقات تستخدم لتعزيز الخصوصية ومنها برامج لإخفاء الهوية . ولكن استخدام التجارة الالكترونية بطبيعته لايسمح بإخفاء الهوية وهنالك نظم أخرى مثل PGP cookie, cutter ويستخدم للتخلص من ال cookies وقد ساعدت فى الجهود التى اضطرت نظم التصفح لتسمح للمستخدمين برفض ال cookies. وعلى أى حال فمن ناحية اخلاقية يجب الحصول على اذن المستخدم قبل جمع معلومات تخصه وعند استخدامها مع توضيح نوع الاستخدام .

سرقة الهوية Identity Theft :-

اساءة استخدام هوية الشخص (اسمه، عنوانه، رقم رخصة القيادة الخ) والغرض القيام بعمل مباح لصاحب الهوية وغير متاح للمستخدم.

التخفى Anonymity:- دخول المواقع دون الكشف عن الهوية. هنالك وسائل تساعد على ذلك Anonymizer . هل التخفى أخلاقى؟ هل بالضرورة أن المتخفى يريد أن يقوم بفعل غير أخلاقى؟

مأزق أخلاقي

استخدام موارد الشركة في التعليم

- أنت مبرمج جديد في شركة وتواصل تعليمك في الجامعة في الفترة المسائية . تستخدم جهاز الكمبيوتر المحمول الخاص بالشركة لأداء الواجبات الدراسية مما يعرض الجهاز للفيروسات حيث أن أكثر الأماكن التي تنتشر فيها الفيروسات هي معامل الجامعة
- هل تعريض موارد الشركة لخطر الفيروسات أخلاقي ؟