سلسلة أوراق

الحق في المعرفة

الخصوصية الرقمية

بين الانتهاك والغياب التشريعي

كريم عاطف

سلسلة ميم: أوراق الحق في المعرفة تصدر عن مركز دعم لتقنية المعلومات

مركز دعم لتقنية المعلومات
2 ش حسين المعمار متفرع من محمود بسيوني - ميدان طلعت حرب - وسط البلد - القاهرة
02 257 56 417 | info@sitcegypt.org | sitcegypt.org

مقدمة

يمكن أن تُعَرف الخصوصية بأنها تَحَكُّم الأفراد في مدي وتوقيت وظروف مشاركة حياتهم مع الآخرين. وتدخل الخصوصية كحق يمارسه الفرد للحد من إطلاع الآخرين على مظاهر حياته والتي يمكن أن تكون أفكاراً أو بيانات شخصية [i].

وقد أدي إتاحة شبكة الإنترنت للجمهور منذ عام 1991 في إحداث نقلة سريعة في مجال تكنولوجيا المعلومات بعد أن كان مُقتصراً على الأبحاث الأكاديمية والعسكرية فقط. كما تَبِع ذلك تطور البرمجيات التي سهلت استخدام الإنترنت فتضاعف مستخدمي الإنترنت من 360 مليون نسمة عام 2000 إلى ما يقارب 2.7 مليار نسمة في عام 2013 [ii]. وتوَسَع استخدام الإنترنت من الأغراض البحثية إلى تقديم خدمات مختلفة للجمهور مثل البريد الإلكتروني والمراسلة الفورية والشراء والبيع عبر الإنترنت. فصار تفاعل الأفراد مع الشبكة أكثر إقتراباً وتأثيراً في حياتهم اليومية. جميعنا يستخدم البريد الإلكتروني وكذلك مواقع التواصل الإجتماعي بصفة يومية ومنا من يقوم بعمليات الشراء بين الحين والآخر؛ وبالتالي أصبح الإنترنت أكثر تماساً مع خصوصيتنا.

ما يسمى "الخصوصية الرقمية" هي وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية. وتتمثل البيانات الشخصية في البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن وكل البيانات التي نستخدمها في تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الإتصال الرقمي بالشبكة العنكبوتية.

ونظرا لتزايد تفاعل الأفراد مع العالم الرقمي أصبحت الخصوصية مهددة وصارت البيانات الشخصية مادة يتم استخدامها إما تجارياً في تنفيذ دعاية تسويقية، أو مراقبتها من قِبل جهات حكومية، أو تعرضها للسرقة واستغلالها في أغراض تضر بأصحابها. وكوْن الحفاظ على الخصوصية الرقمية قضية حديثة العهد فإن التعامل مع التجاوزات التي تؤثر فيها من قِبل الحكومات، أو أية أطراف أخرى تحتاج إلى العديد من التوجيهات عن كيفية حمايتها من خلال تحديث الأطر القانونية ذات الصلة.

سياسة التجسس الرقمي

التجسس، أو "المراقبة" – كما تطلق عليه الحكومات– هي متابعة ورصد لأداء وأنشطة الأفراد في تفاعلهم مع حياتهم اليومية، ويعد استخدام الإنترنت أحد هذه الأنشطة. وقد توّسع استخدام الحكومات للتجسس على مواطنيها أو حتي مواطنين دول أخري مع التطور التقني الذي مر به العالم وذلك طبقا للظروف التي تمر بها هذه الدول وخاصة السياسية منها. فإن كنت تعيش في غضون منتصف القرن العشرين – فيما بعد الحرب العالمية الثانية – فإن مراسلاتك التلغرافية يتم مراقبة الصادر والوارد منها، أما إن كنت تعيش في الفترة ما بين العقد السادس والثامن من القرن العشرين فإن مكالمتك التي تقوم بها من هاتفك الأرضي ستكون عرضة للتنصت[iii]. في منتصف العقد الأخير من القرن العشرين تبنت الحكومات تقنيات أكثر تطوراً لمجاراة انتشار استخدام الهاتف المحمول والإنترنت.

كان لهجمات الحادي عشر من سبتمبر – التي استهدفت برجي التجارة العالمي في الولايات المتحدة الأمريكية – أثراً على تطوير الأجهزة الأمنية لأدوات تجسس على جميع الأنشطة الإلكترونية التي تتضمن البريد الإلكتروني، وتصفح الإنترنت، والتعامل البنكي على الإنترنت، بالإضافة للمحادثات الهاتفية ذلك بحجة مكافحة الإرهاب. وأما عن ضخامة التجسس فإن التفويض الذي أعطاه الرئيس الأمريكي آنذاك جورج بوش لوكالة الأمن القومي، والذي كان محدداً بمدة معينة لمنع أى هجمات إرهابية أخري [iv]، لم يتم إيقاف هذا التفويض حتي الآن (2013) بل تم تطوير آليات أخرى للتجسس، كشف عنها إدوارد سنودن (فني حاسب سابق بوكالة الاستخبارت الأمريكية) لصحيفة الجارديان في يونيو 2013.

برنامج الرقابة المعروف بـ PRISM والذي كشف عنه سنودن يستهدف جمع بيانات جميع مستخدمي خدمات الإنترنت لشركات: Google, Apple, Facebook, Microsoft, Yahoo, AOL, PalTalk في جميع أنحاء العالم. من الملاحظ أن هذه الشركات هي الأكثر انتشاراً بين جميع مستخدمي الإنترنت وذلك لتقديمها خدمات متنوعة تلقي اهتمام من العديد من مستخدمي الإنترنت [v].

الجدول التالي يوضح شركات الإنترنت التي خضعت لبرنامج الرقابة بالاضافة للخدمات التي تقوم بتقديمها، بعض الخانات تحتوي على اسم الخدمة المقدمة في حين اكتفيت بوضع علامة (√) والتي تدل على تقديم هذه الشركة للخدمة مع عدم وجود تسمية لها.

مقدم الخدمة / الخدمة	Google	PalTalk	AOL	Yahoo	Facebook	Microsoft	Apple
البريد الإلكتروني	Gmail		AOL Mail	Yahoo Mail		Hotmail (Outlook)	iCloud
متصفح الإنترنت	Chrome					Internet Explorer	Safari
التواصل الاجتماعي	+Google		About.me		√		
نظام تشغيل	Android					Windows	iOS
المحادثة الصوتية والمرئية	√	PalTalk Messenger	AIM	Yahoo Messenger		Skype Live Messenger	iMessage iChat
مشاركات الفيديو أو الصور	Youtube				√		
تخزين الملفات	Google Drive					SkyDrive	Apple Store

استخدمت عملية التجسس على الأفراد محورين للعمل، **الأول** عن طريق جمع بيانات ضخمة عن الحياة اليومية لمستخدمي الخدمات الموضحة في الجدول السابق –سواء كانوا أفراداً أو شركات – ويتم بتحليل هذه البيانات والتي تساعد على تحديد اهتماماتهم وتوجهاتهم السياسية بناء على مشاركتهم أو الصحفات التي يستخدموها أو عمليات البحث التي يقومون بها. ومن الجدول السابق نكتشف حجم البيانات التي يمكن أن يتم جمعها عن المستخدمين، فعلى الأقل معظمنا يقوم يومياً بفحص البريد الإلكتروني بجانب أحد مواقع التواصل الاجتماعي مثل "فيسبوك". يقوم المحور **الآخر** على متابعة أفراد بعينهم معروف مسبقاً عن أنشطتهم ويتم استهدافهم ومتابعتهم، وقد كشفت تقارير الشفافية التي أصدرتها بعض الشركات الموجودة في الجدول السابق عن طلبات من العديد من الحكومات منها مصر والولايات المتحدة، طالبت بها هذه الحكومات بتسليم بيانات بعض المستخدمين[vi].

لم يكن المواطنين الأمريكيين هم فقط الهدف من عملية التجسس، فبناء على الخدمات المقدمة والتي يستخدمها مستخدمي الإنترنت في العالم على حد سواء، فإن البرنامج قام باستهداف دول أخري على رأسها إيران، وتأتي مصر في المرتبة الرابعة في قائمة الأكثر تجميعاً لبيانات مواطنيها المستخدمين للإنترنت بموجب 7.6 مليار تقرير استخباراتي جمعته وكالة الأمن القومي الأمريكية[vii]

قام باحثين في مجال الحماية باكتشاف رسائل تم ارسالها لناشط بحريني كشفت لهم عن أن هناك أحد البرمجيات والمعروف باسم FinSpy تقوم 25 دولة باستخدامه للتجسس على مواطنيها، كان منها البحرين، أثيوبيا، ماليزيا، المكسيك، مصر، قطر [viii]. ويقوم هذا البرنامج بتسجيل لقطات لشاشات الحاسبات المستهدفة، وتسجيل المحادثات النصية، أو محادثات الصوت والصورة التي تقوم بها برامج المراسلة الفورية مثل Skype والتحكم بالأجهزة المخترقة ونسخ محتوياتها. وقد صرَح المدير العام لمجموعة جاما – المنتجة لهذا البرنامج – بأن مثل هذه الحلول التي تقدمها الشركة للحكومات هي فقط من أجل مراقبة الإرهابيين والتنظيمات الإجرامية التي تهدد المجتمع. إلا أنه من تحليل الظروف التي تمر بها الدول التي قامت باستخدام هذه التقنيات فقد وجد أنها دول تُعاني من تأزم سياسي وترتيب متدني في الحفاظ على حقوق الإنسان.

في حين أن الإنترنت يعتبر فضاءاً رقمياً خارج حدود وسيطرة الحكومات فقد أطلقت العديد من الدول مبادرات للسيطرة عليه، ورغم أن السيطرة عليه تعد مشكلة تجعل حرية التعبير للجمهور مسألة مشكوك في تحقيقها، إلا أن تبني الحكومات لسياسات التجسس عامة – وتحديدا آلية كالتي يستخدمها PRISM– جعلها أحد أسوأ المشكلات التي قد كان من الممكن أن يتنبأ بها الباحثين والمدافعين عن الخصوصية، فإن ما كشف عنه "سنودن" يعد إنتهاكاً بالغاً للخصوصية الرقمية.

تشريعات الخصوصية الرقمية

تستند التشريعات التي تدافع عن الخصوصية على تعريفها كقيمة هامة لدي أفراد المجتمع. ونظرا لحداثة موضوع الخصوصية الرقمية تختلف الأطر التشريعية من دولة لأخرى طبقا للمستجدات التي مرت بها كل دولة، وفلسفتها التشريعية، وكيفية تطبيقها للقوانين والتحولات التي يمر بها المجتمع ومقدرة كل دولة على تبني تعديل لقوانينها بناء على قضايا جديدة تكون خارج اطارها التشريعي.

تهتم قوانين الخصوصية بحماية وسائط نقل المعلومات إما عبر الإنترنت أو الهواتف أو حتي البريد، كما تتضمن الحفاظ على سرية المعلومات الخاصة للأفراد الموجودة في سجلاتهم مثل المعلومات المالية أو الصحية. كما يجب أن تضمن بياناتهم الخاصة التي يتم تداولها من خلال التصفح والتواصل على الإنترنت.

قدم استخدام الإنترنت تحديات مختلفة لموضوع حماية الخصوصية، تختلف أنواع القوانين المختصة بالخصوصية في الفضاء الرقمي فهي تتراوح بين حماية البريد

الإلكتروني، وفرض قيود على نشر بيانات التواصل الاجتماعي، ومتابعة نشاط متصفح الإنترنت والمخالفات للبيانات المحفوظة. وفيما يلي الأنواع المختلفة لقوانين الخصوصية الرقمية:

- **قانون حماية البيانات**: تفرض على الشركات المقدمة لخدمات الانترت والتي تقوم بتخزين معلومات رقمية لعملائها من نشر هذه المعلومات أو مشاركتها مع أطراف أخري دون إفادة من العميل.
- **قانون مراقبة الإتصالات**: تُقيد مراقبة وسائل الإتصال بالإنترنت، والتي تكون في مجال العمل أو الموجودة في الأماكن العامة أو حتي في المنزل.
- **قانون الحماية من جرائم الإنترنت**: تمنع الاستيلاء على الهوية أو سرقة البريد الإلكتروني وكل ما يخص حماية البيانات الشخصية التي يشاركها الفرد أثناء استخدامه للانترنت.

الخصوصية في القانون المصري

بإعتبار أن خصوصية الفرد هي حق يجب أن تكفله الدولة وتحميه، فإنه بإختلاف تشريعات وقوانين الخصوصية يجب أن تكون من أجل غرض أساسي وهو السماح للمواطنين بالتفاعل والتعبير بحرية عن آراءهم بدون خوف أو رقابة من أن كل ما يقولونه سوف يُستغل أو يُفضح.

تأثرت الخصوصية الرقمية في مصر بالفراغ التشريعي الذي يخص قضايا الإنترنت وتداول المعلومات – شأنها شأن دول كثيرة – وعدم وضوح الأطر التي تحمي الحريات الرقمية بصفة عامة والخصوصية الرقمية بصفة خاصة.

يعتقد البعض أنه طالما لم يقم بأي جريمة ولم ينتهك القانون فإنه يتمتع بخصوصية وسرية على حياته الشخصية، ذلك أن تجسس الحكومات على الأفراد طالما تم تبريره بأنه بغرض ملاحقة المجرمين والخارجين عن القانون. وعدم وجود تشريع يحافظ على خصوصية الأفراد سَهَّل ذلك اتباع ممارسات التجسس بدعوي الحفاظ على الأمن القومي وحمايته.

في مارس 2011 حصل المتظاهرين الذين قاموا بإقتحام مبني أمن الدولة المصري على وثائق، كان من بينها عروض أسعار لبرنامج FinFisher مقدمة من شركة جاما لجهاز أمن الدولة المصري [ix]. بالرغم من أن شركة جاما صرحت بأنها لم تكن قد سلمت البرنامج أو قامت بأية تدريبات عليه للجهاز، وأفادت الوثائق في مخاطبات داخلية لجهاز أمن الدولة بأن يلتزم الجهاز بعدم التصريح لأي جهة أجنبية أو محلية باستخدامهم للبرنامج.

لا تتضمن التشريعات المصرية على قانون خاص لحماية الخصوصية الرقمية، لكن رغم أن هناك بعض المواد الدستورية التي جاءت على ذكر الخصوصية، والتي تحدثت بصورة غير صريحة عن الأنشطة الإلكترونية إلا أن ذلك حتي الآن لم ينتج عنه قانون. فما جاء ذكره أنه " لحياة المواطنين الخاصة حرمة، وسريتها مكفولة. ولا يجوز مصادرة المراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الإتصال؛ ولا مراقبتها، ولا الإطلاع علىها إلا لمدة محددة، وفى الأحوال التى يبينها القانون، وبأمر قضائى مسبب" [x]. وأيضا فيما يخص الحصول على المعلومات فإن دستور 2012 قد أورد بأنه "حق تكفله الدولة لكل مواطن؛ بما لا يمس حرمة الحياة الخاصة، وحقوق الآخرين، ولا يتعارض مع الأمن القومي" [xi].

وقد فرض قانون العقوبات عقوبة جنائية على كل من يقوم بجمع صور في أماكن خاصة أو قام بتسجيلات تنتهك حرمة الحياة الخاصة للمواطن [xii]، كما أن هناك قوانين جاءت على حماية البيانات الشخصية لشرائح بعينها كعملاء البنوك، والعاملين، والمرضي كما نصت قوانين العمل، والبنوك، والأحوال الشخصية.

تجارب دولية في تشريعات حماية الخصوصية الرقمية

تضمنت المعاهدات الدولية مواد تحفظ حق الفرد في الخصوصية، وضمان عدم تعرضه على نحو تعسفي أو غير قانوني للتدخل في خصوصياته، أو شئون

أسرته أو بيته أو مراسلاته، على أن يحميه القانون من مثل هذا التدخل أو المساس [xiii].

كما ساهمت الدول الأعضاء بالاتحاد الأوروبي في تشريع قوانينها الخاصة لحماية الخصوصية الرقمية، وساهم الاتحاد الأوروبي ببعض المعايير كانت ضمن الإتفاقية الأوروبية لحقوق الإنسان والتي نصت في المادة الثامنة الخاصة بالخصوصية بأنه "1- من حق أى شخص أن يحصل على احترام لحياته الشخصية والعائلية بالإضافة لمنزله ومراسلاته، كما 2- لا يحق للدولة التدخل في هذا الحق إلا بموجب القانون وما تمليه الضرورة في المجتمع الديمقراطي، وما يمس الأمن القومي أو السلامة العامة أو الاقتصادية للبلاد أو لمنع الفوضي وما قد يضر الصحة والآداب العامة أو لحماية حقوق وحريات الآخرين."[xiv]

وقد أدي ذلك لتوسع مفهوم الخصوصية بالرغم من اختلافات تطبيق القانون من دولة لأخرى، فنجد لدي كل من أسبانيا وألمانيا أشد القوانين حزما، في حين أن أسبانيا أكثر الدول الأوربية التي تسجل شكاوي ضد انتهاك حماية البيانات والأكثر تحصيلا لغرامات ضد انتهاكات البيانات الشخصية [xv].

أما عن دول القارة الآسيوية، فقد قامت سنغافورة في عام 2012 بتشريع قانون لحماية البيانات الشخصية يمنح حماية مدتها عشر سنوات بعد وفاة الشخص [xvi]، كما يعتبر قانون كوريا الجنوبية من أقوي التشريعات في آسيا حيث نصت أحد البنود القانون على حماية صورة وصوت الفرد[xvii].

العديد من دول أمريكا اللاتينية قد شرعت قوانين لحماية خصوصية الأفراد استرشاداً لتوجيهات دول الاتحاد الأوربي وذلك من أجل فتح السوق التجارية معها. فقد قامت الأرجنتين في عام 2000 بتشريع قانونها الخاص لتسهيل التجارة بينها وبين دول الاتحاد الأوربي وكان التشريع مبني على معايير الاتحاد الأوروبي.

أما بالنسبة للولايات المتحدة الأمريكية فإن قوانين الخصوصية بها غير مكتملة وتعاني من فقر تشريعي، فهناك قوانين تغطي البيانات المالية مثل الحسابات البنكية والعناوين [xviii]، وآخر خاص بالرعاية الصحية، كما يوجد لديها أيضا تشريع يلزم المواقع التي تقوم بجمع معلومات عن الأطفال تحت سن 13 سنة بوضع سياسة خصوصية عن كيفية التحقق من موافقة الوالدين أو المسئول عن الطفل عند نشر الأطفال لبياناتهم [xix]. كما يوجد اسهامات غير محددة داخل إطار تشريعي، على سبيل المثال فإن المتاجر الأمريكية لها سياسة ذاتية لحماية عملائها لكن المقاضاة في حالة الإنتهاك لن يقابلها أي عقوبة قانونية والمستهلك لن يجد حلا إلا بعدم الشراء من المتجر.

تبنت بعض المؤسسات صياغة مشاريع قوانين للخصوصية الرقمية طبقاً للتطورات التي تمر بها الخصوصية الرقمية، ففي عام2010 قدمت لجنة التجارة الفيدرالية الأمريكية FTC تقريراً يكشف عن أحقية المستهلكين في منع المواقع الإلكترونية من متابعة سلوكهم في استخدام الإنترنت [xx]. تعتبر النقطة المحورية في مشروع هذا القانون أنه يُقيّد برامج تصفح الإنترنت بإدراج وظيفة لعدم التتبع، كما يقترح بأن تكشف الكيانات التجارية عن الوضع الحالي للبيانات الشخصية التي قامت بجمعها ومع من قامت بمشاركتها.

في يناير 2012 اقترحت المفوضية الأوربية تشريع لحماية البيانات والذي يجعل من حق الفرد أن يطلب من مقدمي خدمات الإنترنت بمسح بياناته الشخصية التي يمكن أن تظهر في محركات البحث وسمي التشريع بـRight to Be Forgotten ، ويحاول القانون المقترح بالسماح للمستخدمين أن يطالبوا شركات مثل تويتر وفيسبوك بحذف بياناتهم الخاصة وكذلك جوجل بأن تمنع من ظهور هذه البيانات في محركات البحث لديها.

استنتاج وتوصية

برغم أن الدول التي تمتلك تشريعات تحفظ خصوصية مواطنيها من تعرض بياناتهم الشخصية للسرقة أو التجسس أو استغلالها في الأغراض التجارية والدعائية، إلا أن هذه التشريعات غير واضحة كما أنها بها العديد من الثغرات القانونية كونها اعتمدت على معايير قديمة ولم تغطي جميع حالات التي تعترض الخصوصية الرقمية.

إن الحكومات التي تقوم بالرقابة على المواطنين بموجب حماية الأمن القومي ومكافحة التنظيمات الإجرامية والإرهابية قد لا تمتلك قوانين تحافظ على الخصوصية، وبالنسبة لحالة القانون المصري فإنه يعتمد على معايير قديمة لا يمكن أن تجاري الظروف الحالية لذا لابد من تحديث هذه المعايير. كما أن الأجهزة الأمنية لا تستخدم في الكثير من الأحيان إذناً قضائياً يسمح لها بالمراقبة، وبذلك ينتهك حق المواطن في معرفة ما إن كان عُرضة للرقابة أم لا، كما يتجاوز حقه برفض ذلك. لذا يجب أن تستند الرقابة على أمراً قضائياً، ويتم متابعتها من قبل هيئة مستقلة عن الأجهزة الأمنية، على أن تضمن هذه الهيئة عدم وجود للبيانات الخاصة للأفراد في نطاق الجهات غير الحكومية وتشرف هذه الهيئة أيضا على تطبيق القوانين التي تحافظ على البيانات الشخصية.

يجب تشريع قانون يحافظ على الخصوصية الرقمية لا يتعارض مع حرية التعبير والخصوصية كما نصت عليه المواد الدستورية، كما يجب أن يُلزم هذا القانون الشركات التي تقدم خدمات الإنترنت والإتصالات بعدم الإحتفاظ بالبيانات الشخصية دون علم صاحبها. كما يجب أن يتم تجريم كل برامج الرقابة الغير قانونية سواء من الجهات الحكومية أو من الشركات الخاصة.

إن أهم ما قد يحافظ على خصوصية الأفرد الرقمية ليس فقط تشريع قانوناً ولكن أيضا ضمان تطبيقه بالإضافة لقابليته للتعديل بناء على ما قد يجد من انتهاكات تمس الخصوصية الرقمية.

المصادر

([i]) Conflicts of Interest, Privacy/Confidentiality, and Tissue Repositories: Protections, Policies, and Practical Strategies Conference co-sponsored by PRIM&R and the Columbia University Center of Bioethics. 2004 May 3-5; Boston, MA

(ii) ICT Facts Figures 2013 - ITU http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

([iii]) Factbox: History of mass surveillance in the United States http://www.reuters.com/article/2013/06/07/us-usa-security-records-factbox-idUSBRE95617O20130607

([iv]) NSA inspector general report on email and internet data collection under Stellar Wind – full document http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection

([v]) المصدر السابق

([vi]) تقرير شفافية أصدرته فيسبوك عن النصف الأول من 2013 ينتهي في 30 يونيو
https://www.facebook.com/about/government_requests

([vii]) Boundless Informant: the NSA's secret tool to track global surveillance data - http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

([viii]) Researchers Find 25 Countries Using Surveillance Software http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/

(ix) ملف خاص بمنتجات برنامج Finfisher -جهاز مباحث أمن الدولة، وزارة الداخلية -http://www.f-secure.com/weblog/archives/finfisher.pdf

(x) المادة 38 من الدستور المصري 2012، المادة 5 من الإعلان الدستوري الصادر في يوليو 2013 -http://egelections-2011.appspot.com/Referendum2012/dostor_masr_final.pdf

(xi) المادة 47 من الدستور المصري 2012

(xii) المادة 309 مكرر من قانون العقوبات 1937

(xiii) العهد الدولي الخاص بالحقوق المدنية والسياسية– المادة 17 http://www.ohchr.org/AR/ProfessionalInterest/Pages/CCPR.aspx

(xiv) Convention for the Protection of Human Rights and Fundamental Freedoms - http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

(xv) Data Protection Laws of the World, March 2013 http://www.thelawyer.com/Journals/2013/03/20/t/b/l/Data_Protection_Laws_of_the_World_2013-414865.pdf

(xvi) Personal Data Protection Act 2012 - REPUBLIC OF SINGAPORE http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A32762ba6-f438-412e-b86d-5c12bd1d4f8a;rec=0;whole=yes

(xvii) FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers http://www.ftc.gov/opa/2010/12/privacyreport.shtm

(xviii) Gramm-Leach-Bliley Act – Bureau of Consumer Protection http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

(xix) Children's Online Privacy Protection Act of 1998 http://www.ftc.gov/ogc/coppa1.htm

(xx)FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers – Federal Trade Commision.