Notas de la Charla en OPEN ZEMOS 2007

Diapositiva 1
¿Por qué seguridad y privacidad? Porque nunca antes como ahora se justifica cualquier medida restrictiva como una medida "por nuestra seguridad". ¿DNI para dormir en un hotel? ¿Cuatro arcos magnéticos para acceder a un avión? ¿100 ml de liquido como límite máximo? Todo eso son medidas que se toman "por nuestra seguridad", luego veremos porqué.

¿Encrucijada? Por supuesto que el desarrollo de internet y lo que se denominan como nuevas tecnologías ha traído grandes ventajas a nuestra vida. Pero tienen un reverso cuyo filo nos puede *cortar* si no se usa bien.

Diapositiva 2
El proyecto: Un weblog, que nació como weblog personal para ir madurando como tribuna de opinión, de estudio y análisis de la nueva sociedad bajo vigilancia en que nos están introduciendo.

El proyecto cuenta como apoyo con un buscador específico que funciona a modo de directorio y que muestra sólo resultados provenientes de páginas que manifiestan una opinión diferente a la que se apoya desde los telediarios y los comunicados gubernamentales.

Para finalizar una contextopedia: Un "wiki" para aclarar términos que se usan en el blog con frecuencia y cuyo significado pueda ser desconocido.

Diapositiva 3
Simple sumario de los contenidos de la charla.

Diapositiva 4

La charla tiene un tono oscuro, a veces puede parecer demasiado apocalíptico. Sirva esta nota para reseñar que esto se debe sólamente a que de las cosas bonitas que la tecnología actual tiene ya se habla mucho, quizá demasiado.

Diapositiva 5
El término privacidad tiene muchos detractores, que lo consideran un anglicismo y por tanto lo denostan. Desconozco si el término proviene del inglés "privacy", que se traduce como intimidad. Pero desde luego, siendo similares, la RAE marca diferencias entre ambos. Siendo ambas, privacidad e intimidad, algo a proteger, vamos a diferenciar entre ambos. Generalmente hablaremos de privacidad, por lo que de derecho a mantener privado tiene.

Diapositiva 6
El problema: En ésta diapositiva queda bastante claro qué supone un problema de privacidad. Éste surge cuando existe la posibilidad de unir un determinado hecho a una determinada persona. Las encuestas anónimas que dicen que "el 10% de la gente prefiere el refresco X frente al refresco Y" no suponen un problema de privacidad, el problema es que alguien (el público en general o la misma empresa que realiza la encuesta) pueda saber qué prefieres tú.

Sólo añadir que el problema de protección de la privacidad no es un problema tecnológico. Es un problema legal. No es que la técnica permita invadir nuestra privacidad, quizá hay formas de ocultarnos. El problema es que la ley debería regular cierto tipo de actuaciones.

Diapositiva 7
Linea temporal de los últimos 250 años. Obviando la era digital, de la que hablaremos más adelante.

Se suele tomar como nacimiento de las democracias modernas las revoluciones francesa y estadounidense. Apenas 200 años de democracias, sólo en occidente y sólo a duras penas (en España lo sabemos bien). Muchos historiadores consideran que este hecho es una casualidad histórica. Opinan que antes no hubo democracias reales como las que disfrutamos en europa, y que con el tiempo el sistema evolucionará hacia algún tipo de sistema totalitario.

Decir que en 2007 todos los países de la UE (excepto UK y Dinamarca) disponen de un equivalente al DNI español. A riesgo de caer en la Ley de Godwin (por primera y última vez en esta charla) diré que éste padrón con esta tarjeta de identidad fue toda la información de que dispuso Hitler para perseguir al pueblo judío. Esto supone mucha menos información, y menos actualizada, de la que nuestros gobiernos tienen de nosotros ahora.

Viviendo en democracia no deberíamos temer nada, pero es que la historia nos enseña que no sabemos qué hay más allá, nadie puede predecir el futuro.

En la misma línea y como pequeño matiz, el DNI fue introducido en España por el régimen fascista y dictatorial de Franco, quien para dar ejemplo se asignó a sí mismo el documento número 1 en marzo de 1944.

Diapositiva 8
La política del miedo.

En 1949, Qutb fue a EEUU (la nueva tierra prometida tras la victoria en la segunda guerra mundial) con el objetivo de estudiar su sistema educativo, y lo que vio allí inspiró una serie de ideas que medio siglo después han devenido en la politización y radicalización del islam.

Lo que en la época de posguerra se percibía como una sociedad alegre, a él le pareció una sociedad en decadencia ética. Vacío personal, y vanalidades (cine, automóviles, …). Materialismo e individualismo estaban pudriendo la sociedad americana y volvió a Egipto para evitar que esta cultura "sucia" se adueñara de su país. La moral nihilista norteamericana amenazaba el correcto desarrollo de una vida acorde a los preceptos del islam.

El medio que ideó para ello fue devolver al islam un lugar preeminente en la política de su país. La "politización del islam". Las ideas de Qutb acabarían teniendo largo alcance, pues el día después de su ejecución (acusado de rebeldía) uno de sus pupilos, Ayman Al-Zawahirí, fundó la Yihad Islámica. Años más tarde, Al-Zawahirí sería mentor y principal influencia ideológica de Bin Laden.

Leo Strauss (filósofo, Univ. De Chicago), compartía la visión de Qutb: América se destruye en su individualismo. Strauss dice que eso se puede detener: "los políticos deben instaurar mitos en los que todos puedan creer; pueden ser mitos falsos si hace falta, pero son –al final - mitos necesarios". Se trata de construir un nuevo conjunto de ideales que hagan recuperar a la gente la fé en sus políticos, bastante débil tras las promesas (nunca cumplidas) de "un mundo

mejor". ¿Os suena eso...?

Dos mitos serán suficientes: Religión, y Nación. En América se tradujo ésto inmediatamente como que era El Pueblo Elegido para combatir a las fuerzas del mal a lo largo del planeta. Uniendo los dos nuevos mitos en uno y usándolos al unísono. De este modo se produjo el mismo efecto que en los paises árabes: La religión se volvía a mezclar con el estado.

Las ideas de Strauss también tendrían largo alcance, ya que pasado el tiempo serían las que inspirarían a los neoconservadores estadounidenses que actualmente ostentan los poderes político y económico de ese país (Rumsfeld, Cheney, Bush padre).

Es importante que la élite destinada a propagar el mensaje no necesitaba, según Strauss, creer en el mensaje. Tan sólo debían hacer lo posible para que la ciudadanía sí creyera, adoptando en público actitudes que guiaran a esa impresión.

Diapositiva 9
Desde los años ’70 en que los conservadores ascendieron al poder, se había promovido la idea de que los movimientos terroristas alrededor del mundo estaban subvencionados por Moscú, que pretendía de este modo sumir al mundo en el caos para apoderarse de él. La caída de la URSS sin la desaparición del terrorismo llevó a la necesidad de reinventar el mito.

Tras años de reestructuración propagandística tenemos ahora una situación similar en la cual se nos presenta una coordinada, pero ya no estaban bajo las órdenes de Moscú, sino del enemigo islamista. Una red de la que casi nadie sabe nada, cuyos líderes nunca son vistos, dudándose incluso de la verdadera identidad de alguno de ellos.

Este cambio de táctica hizo que la otra parte, los seguidores de las ideas de Qutb, que también ganaban adeptos, también reenfocaran su mito: Ahora no es la moral estadounidense la que destruye a los musulmanes, sino los estadounidenses mismos los que destruyen a los musulmanes extendiendo deliberadamente lo que ellos consideraron una enfermedad.

En los últimos años las ideas han sido radicalizadas por uno y otro bando: De los atentados del 11-S al uso de armas químicas en Fallujah (35000 muertos en dos días) por parte estadounidense la guerra "contra el terror" se hace fuerte en los medios, ya que tanto a los conservadores como a los islamistas un conflicto de este tipo le asegura un mayor poder tanto dentro como fuera de su territorio (en tiempos de guerra se pueden pedir cosas que de otro modo serían imposibles de pedir al pueblo).

Diapositiva 10
Es evidente que estos dos grupos han cambiado el mundo, pero no en el modo en que perseguían en un principio. Ambos eran idealistas que rápidamente se dieron cuenta que estas ideas les devolvían el poder que la política tradicional y sus promesas (nunca consumadas) ya no les daba: El poder de conseguir que el pueblo los obedeciera.

La doctrina de la guerra preventiva se hace fuerte y comienza a calar la idea de que para prevenir atentados "desde dentro" hace falta controlar qué hacen los ciudadanos.

Esto no es nuevo, a veces se lee que esto es consecuencia del 11-S. No es cierto. Esto ya estaba decidido desde antes, el 11-S es sólo la excusa esgrimida. Hace 30 años la excusa era el enemigo comunista, ya hemos explicado este punto.

¿Por qué control? Porque es la mejor manera de afianzarse en el poder. Los dos regímenes cuyos ciudadanos han estado más vigilados a lo largo de la historia eran regímenes idealistas, revoluciones populares que se apoyaron en el mismo pueblo para delatar y ajusticiar a posibles traidores. Fueron los regímenes de la URSS y el Chino. El primero tardó casi 80 años en derrumbarse (y sus secuelas aún siguen vivas en Rusia), el segundo no tiene visos de caer. La sociedad China es el claro ejemplo de sociedad bajo vigilancia en el que las nuevas tecnologías se usan para apresar disidentes.

China lleva a cabo el 80% de las ejecuciones mundiales, algunas de las causas que conllevan la muerte ni siquiera implican violencia (evasión fiscal, por ej).

De este modo, las nuevas comunicaciones y las nuevas tecnologías las agrupo en dos conjuntos: El primero lo

denomino "grabándolo todo, en todas partes", y hace referencia a que actualmente es muy difícil decirle algo a alguien y que no quede constancia. Si se lo dices por SMS la persona que lo recibe tendrá una copia, si lo dices por correo-e, chat, mensajería instantánea, telefonía digital... seguramente tu contacto guardará una copia y OBLIGATORIAMENTE tu proveedor de internet lo hará. Es el registro de las comunicaciones y por ley hay que almacenar la traza de las mismas (traza: destinatario, remitente, tipo de conexión y dispositivos empleados). El gran problema es que en internet la traza es indistinguible del contenido, con lo cual no se guarda sólo la traza, sino también todo el contenido.

El segundo grupo son herramientas de control propiamente dichas. Neutralidad de la red (principio que rige internet y que dice que no se puede bloquear el acceso a una web o entre dos computadoras, ya que ello constituye censura y bloqueo a la libertad de expresión e información.

DRM, gestión de derechos digitales. Usualmente se habla de ellos cuando se habla de música en internet, p2p, ... La realidad es que el DRM constituye una amenaza mucho mayor de lo que imaginamos y que puede llegar a determinar qué cada vez que intentamos abrir un archivo o ejecutar un programa nuestro ordenador revise que tenemos permiso (por ejemplo, contactando con un servidor en internet, diciéndole quiénes somos y dónde estamos).

Diapositiva 11
Así tenemos dos visiones del control que se relacionan: De información y de personas.

¿Por qué control? Para perpetuarse en el poder. ¿Alguien duda que si el anterior ejecutivo hubiera podido bloquear las webs extranjeras el 12 y 13 de marzo no lo habrían hecho? Yo opino que la tentación habría sido demasiado fuerte, del mismo modo el actual ejecutivo (de distinto signo político pero con las mismas intenciones perpetuativas) en el nuevo proyecto de la LSSICE ya se asegura de que se puedan bloquear contenidos de internet extranjeros. Justificado con la excusa de bloquear sitios de pedofilia (fin encomiable, aunque más valdría educar a nuestros adultos) permitirá bloquear la BBC si hiciera falta.

Creo que no hay mucho más que decir sobre eso, es aberrante.

El segundo punto es autoexplicativo: Si saben qué haces todo el tiempo (qué comes, cuándo, si bebes cerveza, si duermes poco, ...) podrían denegarte tu pensión, tu ayuda sanitaria (por irresponsable, tú tienes la culpa de tu desgracia). Esto ya ha comenzado a suceder: en Suecia los obesos ya pagan más impuestos (requieren más atención del servicio de salud), Blair es el político que más está avanzando en estas técnicas de control, que está extendiendo en todos los frentes.

Diapositiva 12.
Nuestros derechos, actualmente nuestras normas nos los otorgan (la constitución prevalece sobre cualquier ley estatal) pero no existen normas regulatorias que impidan que estos sean violados. Estamos en el punto de inicio de la charla: El problema de la privacidad es legal, no es técnico (bueno, un poco sí...).

Diapositiva 13.
Factores que ponen en peligro nuestra privacidad, agrupodos según qué aspecto ponen en peligro.

¿Todo puede ser utilizado en tu contra? Me refiero a lo que ya comentamos antes: si todo puede ser grabado, todo puede ser buscado y usado contra tí más adelante, sea cual sea la causa, justificada o no.

Sé que esto puede parecer bueno: Un terrorista podrá ser juzgado. Esto constituye la falacia del político: Vigilar a toda la población es una tarea faraónica, podrás averiguar a posteriori quién planeó qué, pero no evitarlo. Por tanto estos sistemas de vigilancia tienen toda su fuerza cuando con ellas se pretende atacar a un individuo concreto, ya que antes o después se le podrán encontrar "trapos sucios". Esto lejos de ser dejarnos más seguros nos deja en posición de inseguridad. Tan sólo imagínense toda esa información en manos de alguien que te odie a muerte.

RFID, no hemos hablado de ella, luego lo haremos.

Diapositiva 14
Otra visión de los mismos factores, agrupados. De nuevo las dos visiones anteriores, de nuevo relacionadas.

Diapositiva 15
¿Quién sale ganando?
Bueno, lo que llamamos generadores de contenidos (televisiones, discográficas, estudios de cine) son primeros beneficiarios de las restricciones digitales, ya que se impide que le prestes una película a tu hermano, o le regales una copia de tu último cd a tu novio/a. Cada uno debería pagar por el suyo.

Las telecos salen ganando tanto con el DRM como con la neutralidad de la red. ¿Por qué? La neutralidad de la red se rompe priorizando la conexión a las webs de aquellos que más paguen, de modo tal que la teleco cobra POR EL MISMO SERVICIO dos veces: al consumidor y al proveedor original; negocio redondo.

Pero con el auge de la televisión por internet (imagenio y similares, youtube y similares) las telecos ambicionan convertirse además en proveedores de contenidos, de modo que sean ellos los que controlan qué se puede ver, y a qué precios. Ahí les interesa, por supuesto, que estos contenidos no se puedan copiar. Por eso les interesa el DRM.

Absolutamente todos salen ganando con la RFID, que ahora explicaremos en detalle.

Diapositiva 16
RFID: Radio Frequency Identification. Identificación por radiofrecuencias.

Son microchips que emiten radiafrecuencias, por tanto funcionan sin contacto (muchas veces los anuncian como "inteligentes"), como los que se usan para entrar a muchos edificios de empresas. Esto significa que no se usan como la tarjeta de crédito en un cajero, sino que funcionan por proximidad.

La distancia necesaria para activarlo y leerlo varía de un chip a otro, pero es previsible que al avanzar los sistemas de detección y modulación de señales esta distancia se haga cada vez mayor. Cuando están a una distancia especificada del detector (por ej. el cajero, la barra del parking, o la puerta de un edificio) ya puede ser leído.

En principio hay dos tipos de chips: Activos y pasivos. Los pasivos tienen menor alcance y no necesitan baterías ni pilas, porque para funcionar cogen energía de las radiofrecuencias que emiten los detectores de estos microchips. Los activos pueden ser leídos a varios cientos de metros, pero tienen vida limitada a la duración de la batería. Debido precisamente a esto los pasivos son los más usados y también los más peligrosos (pese a su menor alcance) pues no pueden ser desactivados.

Estos chips tienen un número de serie único (una especie de DNI ÚNICO para cada uno): Importante, No es un DNI idéntico para todos los tetrabriks de leche, sino que es un dni distinto para cada tetrabrik de leche ¡Esta diferencia es muy importante y determina que el código de barras no sea un problema pero este código que llevan los chips sí lo sea!

Otro problema añadido de estos chips es que son muy pequeños, no se ven a simple vista con lo cual nuetros zapatos, nuestro jersey, o nuestro llavero podrían llevar uno sin que lo viésemos.

Diapositiva 17
Debido a este carácter único son herramientas de márketing y publicidad impresionantes. Ya que no sólo informan de qué compras (eso ya se sabe cada vez que pagas una compra con una tarjeta de crédito), sino cómo y cuándo lo consumes.

El dispositivo necesario para leer estos chips es muy barato (apenas 50 o 60 euros bastan para coprar los componentes en una tienda de electrónica). Ahora imaginen que sus zapatos llevan uno de estos chips, pocas veces le prestamos nuestros zapatos a otra persona. En el momento de comprarlos el número de serie del zapato se asocia a nuetra tarjeta de crédito, y luego el zapato puede ser leído en cualquier parte, sirviendo para identificarnos. ¿Interesante? Fácil.

¿Realmente hay alguien intentando seguir a personas de esta forma? Sí, IBM ha patentado el sistema. Existe además una empresa dedicada a la fabricación de estos chips para implantes subcutáneos (chips similares a los que hace años son obligatorios para los perros), para hacerlo aún más sencillo.

EPC: código de barras convencional.

UPC: código único de cada producto con RFID

Diapositiva 18
Motivos sobrados. Entre los principales nuestra intimidad: Nuestro hogar es hoy por hoy (y cada vez menos) el único espacio lire de publicidad que tenemos. Con estos chips nuestra nevera sabe cuándo sacamos un producto, y automáticamente podría encargar al supermercado que añada otro igual a nuestra lista de la compra, amén de recomendarnos productos similares si paseamos por el supermercado con uno de estos en la mano.

Por supuesto también están los motivos de privacidad: No damos nuestro número de teléfono a cualquiera pero ahora pueden leer nuestro pasaporte y saber dónde vivimos, nuestra fecha de nacimiento, nombre, apellidos, ... ¿Seguro que queremos?

Al funcionar sin contactos pueden ser leídos a través de nuestro bolso y saber así qué llevamos. "Eso explica que aquel hombre que juega con algo que parece una PDA no deje de mirar el bolso donde llevas tu nuevo Macbook Pro de 2500 euros..."

Diapositiva 19
El pasaporte español incluye chip RFID. El DNI no lo incluye, pero incluye información biométrica que podría ser hackeada en pocos años, menos de los previstos por el gobierno cuando lo creó.

Diapositiva 20
No todos los experimentos sociales en las cárceles son represivos, pero la gran mayoría sí. ¿Por qué? Porque si una técnica de represión es aceptada bien por los reclusos y se los consigue doblegar, sin duda alguna también servirá para controlar a la gran masa de población (mucho más mansa y conflictiva que la población reclusa, en promedio).

De este modo emplear alta tecnología para controlar reclusos no es algo nuevo. Destacamos que hace ya varias décadas que la videovigilancia comenzó a usarse en las prisiones, y sólo en los últimos años (cuando su eficiencia está demostrada para controlar a las personas) dejan las prisiones para invadir las calles. Se aplican así a las personas libres, inocentes mientras se demuestre lo contrario, técnicas de control y coacción.

En la idea de vigilancia vamos a descatar el Panóptico de Bentham, citando Wikipedia:
"Bentham ideó una cárcel en la cual se vigilara todo desde un punto, sin ser visto. Bastaría una mirada que vigile, y cada uno, sintiéndola pesar sobre sí, terminaría por interiorizarla hasta el punto de vigilarse a sí mismo. Bentham se dio cuenta de que "el panóptico" era una gran invención no sólo útil para una cárcel, sino también para las fábricas. Si bien el modelo de Bentham fue criticado (aunque él lo consideraba una genialidad), de alguna forma todas las cárceles, escuelas y fábricas a partir de aquella época se construyeron con el modelo panóptico de vigilancia."

¿Por qué? Porque tanto en cárceles como en fábricas la idea de que "el jefe" o el "vigilante" siempre te van a ver cuando hagas algo incorrecto está interioriada por todos.

Diapositiva 21
Los motivos para oponerse a estas técnicas de control ya deberían estar claros. Me fijo sólo en un detalle: A menudo se diferencia entre derechos y ciberderechos, cuando en realidad son la misma cosa. Cuando una sociedad depende de la conexión a la red, los derechos a la red son indistinguibles de los derechos fuera de la red.

Si hubiera que diferenciarlos diría que "los ciberderechos son los derechos civiles del futuro". Sólo matizando que yo creo que ese futuro, aunque pueda aún hacerse más evidente en los años por venir -seguro que así será- ya está aquí.

Diapositiva 22
¿Cómo luchar contra esto? A nivel personal hablando del tema, a nivel colectivo formando asociaciones de consumidores que nos defiendan, que defiendan nuestros intereses y que exijan y obtengan de los gobiernos una regulación legal de todas estas tecnologías. De modo que no se puedan violar nuestros derechos fundamentales. No se puede desinventar la rueda, la tecnología está aquí para quedarse. Necesitamos leyes que regulen su uso.

Diapositiva 23
¿Y mientras conseguimos las leyes que protejan nuestros derechos?

Acciones poco técnicas: Pues mientras tanto nos queda el boicot a los productos y empresas que apoyan estos usos ilegítimos de la tecnología. Proteger nuestros documentos electrónicos y nuestra intimidad de pasar a ser parte de nuestro "perfil de cliente", algo que conseguimos comprando en efectivo y renunciando al uso de "tarjetas de cliente". Creedme, si la tarjeta fuera para nosotros más rentable que comprar sin tarjeta, el supermercado no nos la daría.

Acciones algo más técnicas: Cifrado de nuestras comunicaciones y uso de software libre a la cabeza de ellas.

Diapisitiva 24
Informarnos, informar. La red. Correr la voz, en nuestros blogs, en donde sea que se trate el tema, hacer que se encienda la bombilla en alguna parte.

Diapositiva 25
Y volvemos al principio. Mi blog hace precisamente eso, transmite un mensaje: Las cosas están cambiando, y no a mejor. Hay que luchar para mantener nuetros derechos.

Diapositiva 26
Conclusiones, están claras, creo.

Diapositiva 27
... una última reivindicación.

Diapositiva 28
Licencia Reconocimiento-Compartir igual.