Biometría al acecho! La maquinaria judicial manifiesta su solidaridad con dos maquinas biométricas

LLAVOR D'ANARQUIA / LA HAINE :: 24/02/2006

Las tres personas acusadas de haber dañado el 17 de noviembre pasado los terminales de control biométrico del liceo (instituto) de la "Vallé de Chevreuse" han sido condenadas. La recogida de datos biométricos contribuirá a reprimir a personas fácilmente localizables y rastreables, dando así poder a la justicia y las grandes empresas para tratar con mano dura a personas "problemáticas"

1.-Castellano.
2.-Català.

1.- Las tres personas acusadas de haber dañado el 17 de noviembre pasado los terminales de control biométrico del liceo (instituto) de la "Vallé de Chevreuse" han sido condenadas a tres meses de prisión con aplazamiento, 500 euros de multa (por la intrusión en el liceo) y 9086 euros por los daños y los intereses (para las máquinas biométricas). Los tres acusados han sido considerados culpables y coautores de los daños. Han decidido apelar a esta decisión.

Se trata de un juicio cibernético. En ningún momento se ha discutido la cuestión central de este proceso: que máquinas como estas no hacen nada en una escuela ni en ningún otro lugar. Los circuitos electrónicos han sido defendidos frente al simple buen sentido.

Este veredicto es un apoyo objetivo a la difusión masiva de esta tecnología, empresa común del estado y de la industria.

Somos de aquellas y aquellos que rechazan resignarse a este estado de cosas.

El colectivo contra la biometría.

Extraemos algunos párrafos interesantes del artículo "Control Biométrico: El necesario debate público", de James C. Ross, del Instituto Elcano.

El contexto de la biometría

Se están creando nuevos modos de integración electrónicos cuya finalidad es reducir la identidad a una serie de características biológicas del cuerpo humano "inequívocas". La división RAND de Seguridad Pública y Justicia define la biometría como "cualquier característica o rasgo personal automáticamente medible, sólido y distintivo que pueda emplearse para identificar o verificar la identidad de una persona". Los sistemas biométricos se utilizan principalmente para identificar, verificar y clasificar la identidad de una persona basándose en características fisiológicas o del comportamiento capturadas y

archivadas en redes informáticas.

En pocas palabras, cualquier muestra biometríca susceptible de ser medida tiene que poder recuperarse y convertirse en un formato digital cuantificable con facilidad. La solidez de la muestra se evalúa mediante la capacidad de variación del material humano básico a lo largo del tiempo como resultado de la edad, heridas, enfermedades, exposición a sustancias químicas, etc.

Preocupaciones

Las tecnologías biométricas -a pesar de sus supuestos beneficios- parecen preocupantes en lo que respecta a la protección de datos, la privacidad de las personas y las libertades civiles.

Las preocupaciones más alarmantes sobre la biometría proceden de sus capacidades integradas de "control de datos". Al paso con el que las agencias estatales y el sector privado progresan en la adopción de soluciones biométricas destinadas a satisfacer las demandas de seguridad, es solo cuestión de tiempo que los objetivos originales de identificación y verificación se amplíen para incluir la utilización de un control biométrico destinado a generar perfiles de personas.

En primer lugar, los sistemas biométricos interactúan fácilmente con la tecnología de las bases de datos, lo que facilita las violaciones de la privacidad y la difusión de datos personales sin autorización, además de hacerlas más perjudiciales.

En segundo lugar, las tecnologías biométricas permitirán con el tiempo realizar un rastreo generalizado, lo que implica la posibilidad de vigilar los movimientos y acciones de una persona en tiempo real o de consultar bases de datos en las que se incluya información acerca de estas acciones. La Cumbre Mundial de la ONU sobre la Sociedad de la Información, celebrada en Ginebra el 10 de diciembre de 2003, puso de manifiesto el potencial y los problemas de estos sistemas obligando a los asistentes a llevar insignias de seguridad, aunque no se les informó de que contenían tarjetas inteligentes integradas y también un sistema de Identificación por Radiofrecuencia (RFID), mediante el cual se podían seguir sus pasos por toda la Cumbre.

En tercer lugar, la identificación biométrica solo es válida si lo es también el proceso inicial de registro. Si, para empezar, una persona utiliza documentos falsos para identificarse, todas las capturas de datos relativas a esa persona en el futuro darán como resultado validaciones falsas [lo que podría se utilizado, por ejemplo, por los servicios secretos].

En cuatro lugar, como quiera que los sistemas biométricos conllevan procesos de control repetidos, para los cuales se necesita no sólo una captura inicial de datos biométricos, sino capturas indefinidas en el tiempo, el "rastro de datos" que deja tras de sí una persona a lo largo de su vida se convierte en una fuente importante de información y, lo que es peor aún, en una forma de autodivulgación de la información. El principal problema que plantea la "captura longitudinal y crónica" de datos biométricos es que las personas no pueden controlar el momento en que se les introduce en el sistema, el momento en que se les rastrea, la forma en que se les incluye dentro de una categoría y para qué fines.

En quinto lugar, otra serie de riesgos potenciales dependen del nivel de normalización o interoperabilidad que hacen posible vincular datos entre bases de datos dispares. Al llegar a conectar "múltiples transacciones [informáticas] gubernamentales, empresariales y de ocio cotidianas", los sistemas biométricos del futuro harán que sea posible reunir un "perfil completo" de los modelos de comportamiento de una persona, y esto abrirá la veda a nuevas formas de discriminación.

En sexto lugar, la eficacia de cualquier sistema biométrico reside en comparar datos biométricos con plantillas previamente almacenadas en una base de datos. Sin embargo, las capturas de datos de Información Personal Identificable (PII) a gran escala son susceptibles de generar una utilización malintencionada de las bases de datos. Las bases de datos y los canales empleados para compartir datos PII son objetivos potenciales de ataques cibernéticos, robo y utilización fraudulenta. Las peticiones de datos PII que puedan realizar otras agencias y gobiernos también pueden poner en peligro la integridad de los sistemas de datos personales.

Rastrear y crear perfiles

Por último, otro motivo de preocupación es la capacidad que tienen los sistemas biométricos para rastrear y crear perfiles, concretamente cuando se emplean junto con microchips RFID. Las técnicas de identificación biométrica aumentan significativamente el potencial para localizar y seguir el rastro físico de las personas y enlazar identidades individuales con modelos de consumo, historiales sanitarios y otros datos de carácter personal. La cuestión del rastreo es relevante en tanto que los sistemas biométricos prometen una elevada precisión, gran eficiencia y una amplia interoperabilidad a un bajo coste. Y es imposible que ello no traiga como consecuencia la adopción generalizada de la biometría en ámbitos públicos y privados que antes no estaban conectados, con la consiguiente multiplicación de puntos de rastreo potenciales. La utilización generalizada de la biometría para rastrear y crear perfiles podría tener como consecuencia:

â€¢ Aumentar la visibilidad del comportamiento de una persona y hacer posible la comparación de ese comportamiento con modelos predefinidos para obtener sospechosos o crear nuevas formas de clasificación de las personas.

â€¢ Exponer a las personas a revelaciones políticas perjudiciales o a difamación, a chantaje, e incluso a extorsión.

â€¢ Expandir la gama de pruebas circunstanciales disponibles para la persecución penal, lo que aumenta exageradamente las posibilidades de emitir sentencias erróneas (aunque los defensores de la biometría señalan que se mejoraría la capacidad de rastrear a un sospechoso hasta la escena del delito).

â€¢ Contribuir a reprimir a personas fácilmente localizables y rastreables, dando así poder a la justicia y las grandes empresas para tratar con mano dura a personas "problemáticas" (como competidores, legisladores, líderes sindicales, denunciadores, manifestantes y activistas, clientes y candidatos políticos).

Conclusión

Los modos de comunicación y de control digitales y electrónicos en las sociedades avanzadas abren nuevas puertas para la vigilancia por parte de entidades públicas y privadas para fines múltiples. Los sistemas de identificación biométrica forman parte de esta extensa "sociedad del control" cuyos flujos de datos ya no se circunscriben a las fronteras de cada país.

En un momento en el que los datos personales que circulan por la red se entrecruzan con los mercados internacionales y las organizaciones supranacionales, se necesita responder a cuestiones importantes sobre el poder, la ciudadanía y los progresos tecnológicos a medida que analizamos las políticas y reglamentos en materia de información para proteger a las personas de violaciones de su privacidad y de nuevas formas de categorización discriminatoria.

Afortunadamente, por el momento no es posible lograr un rastreo perfecto, pero los últimos progresos en biotecnología y en ciencia de la información [unidos a las nuevas legislaciones antiterrorista], apuntan en esa dirección.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

2.-La màquina judicial manifesta la seva solidaritat amb dues màquines biomètriques

Les tres persones acusades d'haver danyat el 17 de novembre pasta els terminals de control biomètric del liceu (institut) de la "Vallée de Chevreuse" han estat condemnades a tres mesos de presó en suspensió de condemna, 500 euros de multa (per la intrusió al liceu) i 9086 euros per els danys i els interessos corresponents (per les màquines biomètriques). Els tres acusats han estat considerats culpables i coautors dels danys. Han decidit apelâ€¢lar la decisió.

Es tracta d'un judici cibernètic. En cap cas s"ha discutit la qüestió central d'aquest procés: que màquines com aquestes no fan res a una escola ni a cap lloc. El circuits electrònics han estat defensats front el senzill bon sentit.

Aquest veredicte és un recolzament objectiu a la difusió massiva d'aquesta tecnologia, tasca comuna de l"estat i la indústria.

Som d'aquells i aquelles que rebutjem resignar-nos a aquest estat de coses.

El colâ€¢lectiu contra la biometria.

_____

https://www.lahaine.org/est_espanol.php/biometria_al_acecho_la_maquinaria_judici