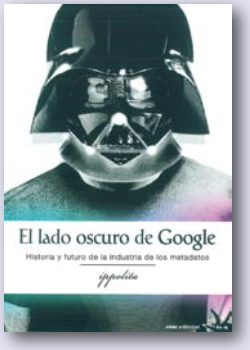


EL LADO OSCURO DE GOOGLE
Historia y futuro de la industria de los metadatos

Autores: Colectivo Ippolita
Editorial: Virus Editorial
Año: 2010 – 205 páginas
ISBN: 978-84-92559-23-7
www.viruseditorial.net

El colectivo Ippolita, un grupo de investigación compuesto por *hackers* y activistas sociales, así como una comunidad de "escribientes" que tiene como fin compartir instrumentos y conocimientos entre el lenguaje del mundo digital y el lenguaje de la escritura, publicó en Internet en 2007 este título que ahora está disponible en formato papel gracias a Virus Editorial.

La presente obra, que tiene como objetivo presentar otras perspectivas menos conocidas del motor de búsqueda ideado por **Sergey Brin** y **Larry Page**, arranca con una breve panorámica sobre la historia de los *search engines*, examinando los momentos más significativos del avance de Google.

La compañía, que ha desarrollado una meticulosa gestión de su propia imagen con lemas como *Don't be evil* ("No seas malo"), siempre se ha cuidado de ofrecer un perfil de "gigante blanco", que los autores de este volumen tratan de desentrañar poniendo en entredicho, por ejemplo, el sistema de asignación de votos y el uso de filtros y criterios no públicos empleados por su algoritmo de indexación de la Red, *PageRank*; el uso selectivo del código abierto para modificar programas cuyas mejoras no hace públicas; la puesta a disposición libre de sus programadores de herramientas que le permiten controlar y apropiarse del trabajo realizado con ellas; u ofrecer a sus trabajadores un 20% del tiempo de trabajo para investigaciones propias, que pasan a ser propiedad exclusiva de la empresa, entre otras polémicas cuestiones.

Asimismo, el libro enfatiza algunas acciones de su agresiva política empresarial, como el fichaje del directivo de Microsoft Kai Fu-Lee, depositario de importantes secretos industriales, la oferta de 50 millones de dólares a AOL a cambio de romper su contrato con Yahoo!, o el paso por alto de varios episodios de censura en distintos países para consolidar su estrategia.

La obra tampoco deja pasar otras cuestiones controvertidas como la falta de privacidad frente al uso de informaciones reservadas para promover una personalización cada vez más cuidada de la publicidad por parte de Google; o la inevitable delgada línea entre lo público y lo privado, dado el ingente volumen de información personal que pasa a través del famoso motor de búsqueda.

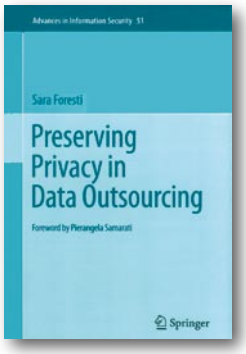
GUERRA EN LA RED
Los nuevos campos de batalla

Autores: Richard A. Clarke y Robert K. Knake
Editorial: Ariel
Año: 2011-367 páginas
ISBN: 978-84-344-6960-0
www.ariel.es

Richard A. Clarke, primer consejero especial para la presidencia de EE.UU. en materia de "ciberseguridad", en 2001, es el artífice de este libro junto a **Robert Knake**, especialista en seguridad nacional y en amenazas transnacionales del siglo XXI. Los autores abren con este título el debate sobre la próxima gran amenaza a la seguridad de los países, la "ciberguerra", de la que dicen "no es una nueva forma de confrontación bélica desprovista de víctimas o limpia, ni algún tipo de arma secreta que sea necesario mantener oculta a la opinión pública, pues es la población civil y las corporaciones de titularidad pública que dirigen nuestros sistemas clave los que con más probabilidad sufran las consecuencias de una 'ciberguerra'".

En este sentido, no se trata de una obra técnica ni un documento militar, sino que desde un lenguaje claro y asequible presenta como punto de partida diferentes enfrentamientos públicos de estados-nación en el "ciberespacio" –como los acaecidos en Siria, Irak, Estonia, Georgia o Corea del Sur– planteando que la imprevisibilidad asociada a la "ciberguerra" a gran escala implica que existe la posibilidad creíble de que un conflicto semejante tenga el potencial para cambiar el actual equilibrio militar del mundo y alterar de forma fundamental las relaciones políticas y económicas vigentes.

En este contexto, los autores proponen asimismo formas de reducir esa imprevisibilidad, desde la perspectiva de los Estados Unidos, como disponer de una estrategia de "ciberdefensa" creíble, fortalecer de forma suficiente las redes importantes que un Estado-nación atacante pudiera querer hostigar, y desarrollar la denominada "estrategia defensiva tríadica" que habrá de emplear la regulación federal como una herramienta importante para definir los requisitos en materia de "ciberseguridad", centrando sus esfuerzos defensivos, al menos inicialmente, en tres sectores: los grandes ISP, como columna vertebral de Internet; la red de suministro eléctrico; y el Departamento de Defensa.



PRESERVING PRIVACY IN DATA OUTSOURCING

Autora: Sara Foresti
Editorial: Springer
Año: 2011 – 180 páginas
ISBN: 978-1-4419-7658-1
www.springer.com

El presente libro ofrece una aproximación completa a la protección de información sensible cuando es almacenada en sistemas que no están bajo el control del propietario de la misma. En este sentido, se dan fundamentalmente tres requisitos de seguridad que hay que considerar a la hora de diseñar un sistema que asegure la confidencialidad de la información almacenada y gestionada: la ejecución del control de accesos para limitar la capacidad de los usuarios autorizados en el acceso a los recursos del sistema; la protección de la privacidad para limitar la visibilidad de la información almacenada/publicada frente a usuarios no autorizados minimizando la adopción del cifrado; y la integración de información segura para limitar la capacidad de los usuarios autorizados en relación con el intercambio de datos para la evaluación de consultas distribuidas.

Con respecto a esta tríada de requisitos, la autora expone en el volumen respectivas propuestas: un nuevo sistema de control de accesos basado en cifrado selectivo que no precisa de un módulo de confianza en el sistema para la ejecución de la política; el modelado de una forma sencilla y a la vez potente de los requisitos de privacidad mediante restricciones de confidencialidad definidas como grupos de datos cuya visibilidad conjunta debe ser evitada; y un modelo para la representación conveniente de las restricciones de intercambio de datos y un mecanismo para su ejecución durante el proceso de evaluación de consultas distribuidas.

Así, su estructura capitular es la que sigue: **1.- Introducción; 2.- Perspectiva del estado del arte; 3.- Cifrado selectivo para la ejecución del control de accesos; 4.- Combinación de fragmentación y cifrado para proteger la privacidad de los datos; 5.- Proceso de consultas distribuidas bajo autorizaciones seguras;** y **6.- Conclusiones.**