Dossier

FUHEM ecosocial

Estado de excepción y control social

Santiago Alba Rico
Alejandro Segura Vázquez
Jean-Pierre Garnier
Ben Hayes
Tica Font

Recopilación de experiencias:
Lucía Vicent Valverde

Selección de recursos:
Susana Fernández Herrero

Dossier

Estado de excepción y control social

Santiago Alba Rico
Escritor

Alejandro Segura Vázquez
Investigador y profesor colaborador de la UNED

Jean-Pierre Garnier
Sociólogo urbano

Ben Hayes
Investigador del Transnational Institute y de Statewatch

Tica Font
Directora del Institut Català Internacional per la Pau (ICIP)

Coordinación: Nuria del Viso
Edita: FUHEM
C/ Duque de Sesto 40, 28009 Madrid
Teléfono: 91 431 02 80
Fax: 91 577 47 26
fuhem@fuhem.es www.fuhem.es

Madrid, 2015

FUHEM Ecosocial es un espacio de reflexión crítica e interdisciplinar que analiza los retos de la sostenibilidad, la cohesión social y la democracia en la sociedad actual.

La ‘Gran Involución” está alcanzando en su deriva el ámbito de derechos, libertades y garantías en el estado español. Al nivel global, un renovado empeño en un concepto mermado de la seguridad se traduce en nuevas formas de vigilancia, control social y represión de la disidencia, a menudo a través de las tecnologías de la información y la vigilancia virtual de la ciudadanía, el uso del espacio urbano para imponer el "orden", perspectivas de toda una nueva generación de armas capaces de atacar de forma autónoma y, sobre todo, el miedo.

Estos son los temas que abordan las firmas incluidas en este dossier: **Santiago Alba Rico, Alex Segura, Jean-Pierre Garnier, Ben Hayes** y **Tica Font**. El documento recoge también algunas experiencias de organizaciones en respuesta a la sociedad vigilada, recopilado por **Lucía Vicent**, y una selección de recursos sobre esta problemática, elaborado por **Susana Fernández**.

FUHEM Ecosocial
Enero de 2015

Sumario

Miedo, contagio, resistencia

Santiago Alba Rico
Escritor

El miedo original

Según la concepción clásica de Sigmund Freud, la 'cultura" es un minucioso dispositivo disciplinario que evitaría la irrupción destructiva de todas esas fuerzas oscuras (el instinto de muerte asociado al placer suicida) que están siempre a punto de saltar sobre el mundo. La 'cultura" salva al mismo tiempo a los individuos, amenazados por un terrorífico deseo asentado en las profundidades, y a las sociedades, amenazadas por estas acucias que acechan desde abajo, como caimanes, para asaltar en cualquier momento la civilización.

La idea de que el peligro está en cada uno de nosotros y la salvación en la sociedad es muy antigua; y va asociada a un pesimismo antropológico que –de Hobbes a Freud– considera que el desorden, la violencia y el caos proceden siempre del 'individuo natural", al que habría que domesticar o, al menos, reprimir en la horma institucional. No es una tontería. Si no es seguro que la guerra sea el resultado de una pulsión de muerte universal, sí es la ocasión de una liberación de libidos destructivas que convierten a cada ser humano en un potencial asesino. Pero esta es solo una visión parcial. Porque cabe interpretar también la historia, en cuanto que historia de la lucha de clases –y cada sociedad histórica concreta–, como el conjunto limitado de las voluntades individuales hegemónicas que reprimen sin parar, y descomponen, la voluntad colectiva. Es decir, cabe pensar la guerra como una pulsión de muerte universal; pero cabe pensarla asimismo como un proyecto particular cuyo propósito es desbaratar el empuje de un proyecto general civilizatorio. Cabe pensar, en definitiva, el poder político como la victoria de unos poquitos seres humanos sobre esa mayoría articulada que estaría buscando el establecimiento de un orden colectivo más estable y más sensato. O lo que es lo mismo: parece razonable suponer que es el poder político, como programa de una clase o un grupo concreto, el que introduce el desorden individual, la violencia y el caos.

El miedo ha existido siempre y es inseparable de la condición humana y de la conciencia de la muerte. Las sociedades son máquinas muy sofisticadas que piensan por nosotros, nos ofrecen respuestas manufacturadas y nos impiden vivir de manera metafísica; es decir, nos impiden autodestruirnos a fuerza de pensar nuestra propia

debilidad. Pero las sociedades son también el material que los gobernantes deben gestionar para imponer sus propios intereses, que raramente coinciden con los de los humanos socializados. En definitiva, el miedo es uno de los recursos fundamentales utilizados desde el principio de los tiempos para impedir una rebelión o, por lo menos, una reacción disonante. Como dejaron claro los tunecinos y egipcios en 2011, toda rebelión es, antes que nada, una victoria sobre el miedo: 'temednos, ya no os tenemos miedo", gritaban en La Qasba y en Tahrir.

Bárbaros y fronteras

Si dejamos a un lado el terror, instrumento pedagógico de 'excepción" –escuadrones de la muerte, bombardeos indiscriminados, tortura, etc.– mediante el cual poderes abiertamente inicuos han afirmado o impuesto tradicionalmente su dominio, podemos decir que la administración del miedo forma parte de la normalidad capitalista incluso en las sociedades democráticas. Ese miedo, como hemos indicado, puede ser de dos tipos: exterior e interior. Añadamos enseguida que la llamada globalización, a través del consumo y de las nuevas tecnologías, ha fragilizado esa frontera, de manera que cada vez es más difícil saber si las amenazas que gestionan nuestros gobernantes proceden de dentro o de fuera porque estas dos categorías se cruzan de manera creciente en nuestros cuerpos, nuestros territorios y nuestros deseos.

El miedo a una amenaza exterior se conoce con el nombre de 'barbarie", frente a la cual se establece el *limes* –la frontera romana– como garantía de supervivencia civilizada, pero también, de algún modo, como ilusión de civilización. El miedo a que los 'bárbaros", semihumanos que no hablan nuestra lengua, que apenas emiten sonidos inarticulados, derriben el muro protector (pensemos en dos obras clásicas como *El desierto de los tártaros* de Buzzati o *Esperando a los bárbaros* de Coetzee) y desbaraten nuestro orden civilizado, maten a nuestros niños y violen a nuestras mujeres, ha servido siempre para conferir una falsa homogeneidad a sociedades frágiles o amenazadas de implosión. El caso contemporáneo más evidente es Israel, un Estado reciente y artificial, impuesto mediante las armas, que necesita de la violencia contra un enemigo exterior amenazante para afirmar su existencia. El 'bárbaro" es una función de supervivencia identitaria de las sociedades debilitadas y una fuente de legitimidad interna de los regímenes cuestionados. Somos civilizados solo frente a los bárbaros que, como decía Anatole France, de 'nosotros los civilizados solo conocen nuestros crímenes".

Como sabemos, en el llamado occidente democrático, el comunismo cumplió esta función barbárica y legitimadora durante décadas. La popularidad del género cinematográfico de ciencia-ficción, en el que malvadísimos extraterrestres, muy evolucionados desde el punto de vista tecnológico pero de físico inquietante o nauseabundo, subrogaban la amenaza soviética, da buena cuenta de este uso político

legitimador de la figura del bárbaro. Pensemos en los grandes clásicos del género, desde *La guerra de los mundos* (1953) a *Independence day* (1996), celebración patriótica de la victoria estadounidense en la Guerra Fría. El placer de saberse amenazado desde el exterior es inseparable del placer de saberse moral y culturalmente superior, matriz de la xenofobia y el racismo.

Tras el final de la Guerra Fría, el bárbaro se islamiza y, como ocurre en la inquietante *Alien, el octavo pasajero* (1979) se instala a vivir en la nave de la civilización; la amenaza adopta la forma del 'terrorismo". Este cambio se produce, en efecto, en un mundo ya transformado, en el que la globalización impone intercambios generalizados y suscita formas de resistencia postmodernas y desterritorializadas. Al-Qaeda, reemplazada hoy por el Estado Islámico, es el paradigma de la barbarie global –franquicia mundializada, como el MacDonald's– que hace inútiles las fronteras y que alarga su sombra en la figura del bárbaro interior; es decir, el inmigrante, prolongación intestinal del yihadista exterior. La guerra impone como naturales las medidas de excepción; pensemos, por ejemplo, en los ciudadanos de origen japonés encerrados en campos de concentración estadounidenses durante la Segunda Guerra Mundial. Pues bien, la 'guerra contra el terrorismo" ha normalizado la excepción jurídica en forma de leyes antiterroristas incompatibles con el Estado de Derecho, al tiempo que ha convertido a los ex-colonizados, hoy inmigrantes clandestinos o irregulares en las metrópolis, en fuentes de amenaza permanentes contra los que hay que levantar también fronteras internas, muros íntimos que alimentan el individualismo en la vida privada y la intervención estatal en la vida pública. El inmigrante criminalizado como terrorista potencial y bárbaro irredimible induce contracciones identitarias (fijémonos en el aumento del fascismo en toda Europa) y zapa sin parar la articulación de formas colectivas de lucha y resistencia frente a la gestión política y económica del capitalismo en crisis.

Esta interiorización del bárbaro, que ahora está entre nosotros, nos convierte paradójicamente en una sociedad bárbara o, al menos, 'primitiva", incapaz de distinguir entre delito, pecado y enfermedad. No es una casualidad que el extraterrestre haya dejado su lugar al zombi, el familiar que se vuelve extraño ('siniestro" lo llamaba Freud), el muerto inmortal que todos llevamos dentro y que, además, como el portador del VIH o del ébola, contagia su inmortalidad caníbal. El zombi, cuyo aspecto semidescompuesto evoca al leproso medieval, excluido y amenazador, cierra esta recategorización del bárbaro que acompaña a la globalización y que asocia de nuevo, como en el pensamiento 'salvaje", cuerpo, pobreza, contagio, violencia, delito. El inmigrante, en general musulmán y potencialmente terrorista, traslada en su cuerpo excesivo el germen mortal que, bárbaro impersonal, se difundirá en nuestras ciudades, destruyendo sin explosiones la civilización y generalizando el caos y la violencia social. El bárbaro es pestífero, pero la peste, a su vez, es la barbarie total.

En efecto, incluso en el imaginario cinematográfico y cultural la Epidemia prolonga la amenaza del bárbaro exterior y del bárbaro interior, combinando ambas en una inhumanidad inasimilable con la que toda negociación es inútil y contra la que toda defensa es imposible. Contra los hombres se levantan muros, se erizan alambres, se despliegan eufemísticas y mortales 'concertinas", pero los virus, como el dinero y las mercancías, cruzan todas las fronteras. De hecho, puede decirse que la pandemia es el reverso tenebroso –todo tiene un reverso tenebroso– del mercado. Y por eso la gestión sanitaria se ha convertido en un elemento fundamental de lo que Foucault llamaba biopolítica; es –aún más– lo que convierte la política en fobiopolítica de la vida y de la muerte. Como hemos visto –estamos viendo– en relación con el virus del ébola, que viene de África, al igual que los inmigrantes y el terrorismo, la administración del miedo sanitario como instrumento de regulación social puede generar incluso crisis de gobierno en las metrópolis porque es inseparable ya de la gestión económica de los mercados. En definitiva, la Epidemia es condición, consecuencia, función y disolución de la globalización capitalista; es el paradigma de un mercado individualista biologizado en el que el otro mismo comparece siempre como amenazante e inhumano y, frente al cual, el poder económico y político se yergue como intervención salvífica y nunca como responsable o causante de nuestros males. De un lado hay un bárbaro interiorizado que puede golpear en cualquier momento; del otro un gobierno cuya única misión es evitar el fin del mundo. Si algo reprochamos a nuestros políticos es que no nos salven, que no sean capaces de salvarnos. De esta manera la crisis del ébola –como antes la de la gripe aviar o la de las vacas locas– revela un orden social en el que la política, entendida como garantía colectiva de la ciudadanía y sus derechos inalienables, es sustituida por una cuarentena o profilaxis ininterrumpida que desarticula toda acción común, ontologiza negativamente a los otros y legitima leyes de excepción contra las libertades y derechos fundamentales.

La interiorización económica del mal

El bárbaro interior globalizado, cuya figura de ficción es el zombi, cuya figura 'corporal" es el enfermo contagioso, expresa el terror individual y social a dejar de ser uno mismo; el miedo a *convertirse en otra cosa*. Parafraseando aquí las reflexiones ya clásicas de la antropóloga Mary Douglas,[1] podríamos decir que la profilaxis y la xenofobia, con la contracción identitaria concomitante, son respuestas desplazadas o fraudulentas a una amenaza cada vez más indefinida e impersonal que se replica de manera viral y que ningún muro puede contener. La renovada afirmación de la identidad nacional, religiosa y cultural es indisociable del miedo al contagio, del rechazo del inmigrante, del temor hipocondriaco frente a la delincuencia y el terrorismo, de la negación del cuerpo y sus procesos biológicos –enfermedad, envejecimiento, obesidad.

[1] Mary Douglas, *Pureza y peligro*, Siglo XXI, Madrid 1973.

Pero junto a este miedo, políticamente muy rentable, está otro directamente vinculado al mercado laboral y a la gestión económica y que se presenta a contrapelo del anterior, pero entretejido con él. Me refiero al miedo a *seguir siendo uno mismo*, el terror a la identidad biográfica, profesional, ética, humana, que puede dejarnos fuera del mercado. No podemos seguir siendo nosotros mismos si queremos seguir trabajando, renovar nuestro contrato, no perder comba frente a una economía en crisis que abarata las competencias y aumenta las exigencias. Es, si se quiere, *el miedo al fracaso* como regulador subjetivo de un capitalismo cuya presión objetiva es asumida por los perdedores, los desechados, los excluidos, como una irregularidad pecaminosa. Privatizar las ganancias, socializar las pérdidas quiere decir también subjetivizar las últimas –las pérdidas– como una disfunción idiosincrásica del perdedor. El naufragio antropológico del ser humano bajo la licuadora del capitalismo se corresponde, porque es su causa, con la emergencia de un individuo autorreferencial, culpable de su propio naufragio, y asustado. El fracaso es un pecado, un delito y una enfermedad mortal.

Hace poco una amiga que trabaja como directiva en una potente empresa editorial me pedía que imaginara la situación de los empleados subalternos y de los trabajadores precarios a partir de las presiones que ella, en la zona alta de la pirámide, experimenta. A una base salarial más bien baja, me contaba, la empresa añade un 'bonus" muy apetitoso condicionado a la consecución de unos objetivos económicos… imposibles de lograr. Cuando ella objetó, en efecto, la imposibilidad de obtener para la empresa los beneficios propuestos, la respuesta adoptó la forma de uno de los eufemismos empresariales favoritos para alentar y justificar la sobre-explotación inmanente del trabajo: 'claro, es un reto". El mecanismo es infalible: el directivo trabaja muchas más horas de las que figuran en contrato sin necesidad de latigazos y la empresa se ahorra una y otra vez el pago del bonus, obteniendo sin embargo altísimos beneficios gracias a esta interpelación a la autosuperación personal (concepto que sustituye al del 'honor" antiguo y medieval). El hecho de que se trate de un 'reto individual" implica además que el trabajador viva la no consecución de un objetivo imposible –y que se sabe imposible desde el principio– como un fracaso personal y, por lo tanto, con culpabilidad. La empresa se pone a salvo así de acciones políticas concertadas o de iras colectivas. La cólera y la frustración se vuelven sobre uno mismo, incapaz de superar la propia incompetencia y de adaptarse a las necesidades cambiantes del mercado.

Podemos imaginar, en efecto, los devastadores efectos políticos que este 'miedo al fracaso" genera en una sociedad con un 25% de paro (más de un 60% en menores de 30 años), con más de un 90% de trabajadores precarios o con contratos discontinuos o a tiempo parcial (y un 13% de ellos en riesgo de pobreza) y con un 20% de trabajadores que tienen la sensación de ser subestimados o infravalorados en sus tareas. Este mecanismo de subjetivización de la crisis y de la sobre-explotación aparejada, que es también el del 'hombre endeudado" y el del 'emprendedor" que se emplea a sí mismo,

convierte el miedo y la culpa en un regulador espontáneo del mercado laboral, sin chirridos ni conflictos sociales. La despolitización del conflicto, asumido ahora en forma de culpa individual, tiene como consecuencia, por ejemplo, la psiquiatrización creciente de los sujetos así separados de sus compañeros o vecinos, con el consiguiente aumento de las consultas y tratamientos farmacológicos. Basta un dato: solo en la primera década de este siglo el consumo de antidepresivos aumentó en un 81% y el de ansiolíticos en un 11%. En los últimos cinco años, el número de consultas psiquiátricas en la Seguridad Social ha aumentado en un 20%. Como bien anticipaba el psiquiatra asturiano Guillermo Rendueles hace diez años, 'la experiencia de la explotación se ha personalizado" y 'el mundo del trabajo contemporáneo está dominado por una concepción de las relaciones laborales semejante a la vivencia del mal típica de las películas de terror de serie B". Esta psiquiatrización de la vida laboral –y del curso entero de la vida– es inseparable, dice Rendueles, de las exigencias de una sociedad capitalista y de un mercado laboral que 'nos exigen estar eternamente disponibles para el cambio", pero también, por ello mismo, del abandono de las luchas colectivas, la mejor protección imaginable contra la ansiedad o la depresión.[2] En este sentido, el 15M fue una socioterapia intensiva –un amigo hablaba en 2011 en Túnez de 'zaurateraрia", de la palabra árabe 'zaura", revolución– cuyos efectos saludables sobre la población estamos empezando a percibir.

De este 'miedo al fracaso" se ha ocupado muy recientemente el periodista Esteban Hernández en un libro muy recomendable, *El fin de la clase media*, en el que analiza con rigor y brillantez el desmantelamiento por parte del mercado y sus 'exigencias de cambio" de esa franja social que el capitalismo había utilizado históricamente como garantía de estabilidad. La crisis, que es también una crisis de los valores característicos de la clase media (la confianza en las instituciones y en el futuro, el trabajo bien hecho, la posibilidad de mejorar, la transmisión de valores y saberes), franquea el espacio a una potencial explotación del miedo, que es siempre conservador (al contrario que el mercado, antipuritano y subversivo), por parte de proyectos destropopulistas o fascistas, tal y como estamos ya viendo en toda Europa. El conservadurismo de clase media, sin embargo, no es inmediata y necesariamente de derechas; pero lo será, sin duda, si la izquierda, apunta Hernández, lo desprecia como reaccionario o contrarrevolucionario.[3]

¿Qué hacer, en definitiva, con el miedo? El miedo puede ser paralizador, pero también movilizador. Si es conservador –esa es la tesis de mi último libro–[4] lo es también frente a un capitalismo que revoluciona todos los vínculos sociales y se desprende radicalmente de toda estabilidad humana. La izquierda debe ser, por tanto,

[2] Guillermo Rendueles Olmedo, *Egolatría*, KRK Ediciones, Madrid 2004.
[3] Esteban Hernández, *El fin de la clase media*, Clave Intelectual, Madrid 2014.
[4] Santiago Alba Rico, *¿Podemos seguir siendo de izquierdas? Panfleto en sí menor.* Pol.len Ediciones, Barcelona, 2014.

conservadora (en términos ecológicos y antropológicos) y poner el miedo autogestionado al servicio de esta obra imprescindible, impostergable, de detención de la revolución capitalista y transformación liberadora de las condiciones de producción, distribución e intercambio de bienes y discursos. Solo entonces el miedo a la muerte, y las supersticiones que produce, será libre, metafísico y relativamente inofensivo.

Digitalizar y controlar: un *collage* de tecnologías vigilantes

Alejandro Segura Vázquez
Investigador y profesor colaborador de la UNED

El control y las nuevas máquinas

Who Controls The Control Men	*Controls Men Control Who The*	*Control Who The Men Controls*
Who Controls The Men Control	*Controls Men Control The Who*	*Control Who The Controls Men*
Who Controls Control Men The	*Controls Who The Control Men*	*Control Who Men Controls The*

Lo que ustedes acaban de leer justo arriba es «Pistol Poem No. 2» de William S. Burroughs. Se trata tan solo de un pequeño extracto; el poema completo se extiende hasta las cuarenta líneas, ordenadas así, como ven, en tres columnas. Ciento veinte frases en total y en cada una de ellas las mismas palabras, desordenadas así, como ven.

Tomando la expresión de Juvenal, *Quis custodiet ipsos custodes?,* Burroughs juega de manera singular a combinar todas las posibilidades de la traducción inglesa y ofrece una composición enigmática. Una composición donde la pregunta «Who controls the control men?» se revuelve sobre sí misma como si fuese una enredadera que serpentea paredes y verjas para asomarse a un afuera aún más intrincado. Como si sus palabras –*who, control, men…*– al intercambiar sus posiciones, alumbrasen de un solo golpe todas las perspectivas de un *collage* de miradas vigilantes que se cruzan.

La imagen lograda por Burroughs evoca una desconcertante alternancia vigilante-vigilado e ilustra una sociedad complicada en la difuminación de sus *locus* de control.[5] No en vano, la lectura del norteamericano ejerce una intensa influencia en la continuación que Guilles Deleuze hará del trabajo de Michel Foucault –quien también sentían una gran admiración por Burroughs– para describir el paso de las *sociedades disciplinarias* a las *sociedades de control*.[6] El brillante descifrado *foucaultiano* de una historia según la cual el poder afloja progresivamente el dominio sobre los cuerpos en favor de sutiles mecanismos de acción sobre las mentes encontró así una de sus

[5] La técnica empleada por Burroughs en esta composición se conoce como *cut-up*: el texto es aleatoriamente recortado y reordenado. Curiosamente Burroughs pensaba que la aplicación de esta técnica permitía prever el futuro, ya que creía que este se filtraba al cortar las líneas de palabras.
[6] Generalmente su novela *El Almuerzo Desnudo (1959)* es considerada la obra más influyente a este respecto.

mejores prolongaciones en una interpretación *deleuziana* que bebía directamente de la noción de 'control" de Burroughs.[7]

Tal y como explica Foucault, a partir del siglo XVIII, la interiorización de las disciplinas precisó lugares de reclusión bien definidos (la escuela, la fábrica, la prisión…) en torno a cuya vigilancia se erigió todo un 'arte" de la representación del orden social.[8] Pero para Foucault, como también señala Deleuze, aquello no era más que la descripción de lo que poco a poco dejábamos de ser.[9] Avanzada ya más de una década del XXI, los dispositivos vigilantes siguen siendo una referencia ineludible de ese orden; sin embargo, más allá de las instituciones de encierro, estos dispositivos se han ido reconfigurando al entrelazarse con el desarrollo de tecnologías informáticas que procuran formas de control más sofisticadas. El castigo, la cárcel, las disciplinas y su interiorización conviven ahora con un control abierto, insidioso y continuo habilitado por la paulatina digitalización de los espacios en los que nos relacionamos.

Sin duda que resultaría reduccionista atribuir exclusivamente a las 'nuevas máquinas" la autoría de este dibujo, pero estas herramientas confluyen de algún modo con toda una colección de factores psicológicos, sociales, políticos y económicos para configurar el ambiente invisible en el que nos desenvolvemos.[10] Se trata de abordar aquí, concretamente, la manera en que nos relacionamos con las *tecnologías de la comunicación digital* y en qué medida, al hacerlo, las modulamos y somos modulados por ellas.

Y es que, aunque no quede agotada en ello, el desarrollo tecnológico remite directamente a una multiplicidad de posibilidades de vigilancia que contribuyen a alimentar la noción de control presentada. La ubicación por satélite de nuestro *smarthphone*, los chips RFID, los *drones*, el reconocimiento facial biométrico, la huella que dejamos en cada operación con nuestra tarjeta de crédito, las redes de espionaje masivo, la minería de datos o algo tan aparentemente trivial como acceder al estado de un contacto de *whatsapp* para comprobar su última conexión; son solo algunas de las incontables evidencias que dan testimonio de lo que Armand Mattelart ha llamado «un mundo vigilado».[11] Esta amalgama de comportamientos y tecnologías parece ir tejiendo una malla social vigilante que extiende el control en múltiples direcciones, penetra en múltiples capas y, por tanto, dispara nuevas concepciones.

[7] G. Deleuze, «Posdata sobre las sociedades de control», en C. Ferrer (ed.), *El lenguaje libertario. Antología del pensamiento anarquista contemporáneo*, Altamira, Buenos Aires, 2000.
[8] M. Foucault, *Vigilar y castigar*. Siglo XXI, Madrid, 2009.
[9] G. Deleuze, *Op. cit.*
[10] Véase M. McLuhan y Fiore. Q, *El medio es el masaje. Un inventario de efectos*, Paidós Studio 65, Barcelona, 2013.
[11] A. Matterlart, *Un mundo vigilado*, Paidós Ibérica, Barcelona, 2009.

La subversión de la vigilancia

Los estudios sobre la vigilancia no han permanecido ajenos a este tejido incipiente y la metáfora de un 'ojo único" que todo lo ve ha ido perdiendo fuelle para dar cuenta de una realidad que se aparece cada vez más poliédrica. El *panóptico* de Bentham,* que sirviera de modelo a Foucault en su descripción del papel de la vigilancia en las sociedades disciplinarias, se ve reformulado para las sociedades de control en distintas formas que constatan que el vigilante se ha desplazado definitivamente del centro para mezclase con un vigilado cuyo lugar ya no está reservado al contorno. El método de inspección que regulaba una jerarquía vertical para disciplinar los cuerpos y las mentes da paso así a un ramillete de formas descentralizadas y horizontales que implica a sus protagonistas en una continua alternancia de roles. Así, Mark Poster emplea el término *superpanóptico* para referirse a una extensión que, más allá de los lugares de encierro, comprende todas las actividades de la vida.[12] Por su parte, Thomas Mathiesen habla de *sinóptico,* enfatizando con ello cierta reciprocidad en los procesos de vigilancia, es decir, esa observancia mutua que expresábamos arriba como alternancia de roles y que abarca también al conjunto de nuestras prácticas relacionales.[13]

En este orden de cosas, topamos además con una realidad paradójica en la que las mismas tecnologías que son distribuidas a la población en el marco de una racionalidad gubernamental determinada, pueden ser empleadas por esa misma población para interpelar dicho marco. Pensemos, por ejemplo, en como un teléfono móvil puede servir a la policía para ubicar la localización de su propietario y, al mismo tiempo, ser empleado por este último para fotografiar o grabar un acto de violencia policial y ponerlo a circular en la red. Esto es una muestra de lo que Milton Santos ha llamado *contrarracionalidades*: usos subversivos de la tecnología.[14] En una línea similar podríamos encuadrar también el término *sousveillance,* propuesto por Steve Mann para describir la observación desde 'abajo" en contraposición a una concepción clásica de la vigilancia desde 'arriba".[15]

---

* El panóptico es un tipo de arquitectura carcelaria ideada por el filósofo utilitarista Jeremy Bentham hacia fines del siglo XVIII. El objetivo de la estructura panóptica es permitir a su guardián, guarnecido en una torre central, observar a todos los prisioneros, recluidos en celdas individuales alrededor de la torre, sin que estos puedan saber si son observados. El efecto más importante del panóptico es inducir en el detenido un estado consciente y permanente de visibilidad que garantiza el funcionamiento automático del poder, sin que ese poder se esté ejerciendo de manera efectiva en cada momento, puesto que el prisionero no puede saber cuándo se le vigila y cuándo no. Fuente: Wikipedia. N. del E.

[12] Véase P. Rodríguez, «¿Qué son las sociedades de control?», *Revista Sociedad*, n° 27, pp. 177-192, 2008.

[13] T. Mathiesen, «The viewer society: Michel Foucault´s Panopticon revisited», *Theoretical Criminology*, n° 1, pp. 215-234, 1997.

[14] Véase L. Melgaço, «Security and Surveillance in Times of Globalization: An Appraisal of Milton Santos' Theory», *International Journal of E-Planning Research*, Vol. 2, n°4, pp. 1-12, October-December 2013.

[15] S. Mann, «Sousveillance: Inverse Surveillance in Multimedia Imaging» *Proceedings of the 12th Anual ACM International Conference on Multimedia,* ACM, pp. 620-627, 2004.

Recientemente diversos acontecimientos de los que se han hecho eco los medios pueden ser interpretados a la luz de estas consideraciones. Edward Snowden, el soldado Manning o Julian Assange son algunos de los nombres propios de esas historias. Snowden, antiguo empleado de la Agencia de Seguridad Nacional (NSA), destapó la existencia del programa secreto de espionaje PRISM por el que, entre otras cosas, el Gobierno estadounidense establecía acuerdos con los gigantes de la red (Google, Facebook, Microsoft, etc.) para obtener información de sus usuarios. En su caso, Manning, analista de inteligencia del ejército de EEUU, proporcionó a Wikileaks documentos confidenciales sobre las guerras de Afganistán e Irak y cables diplomáticos secretos. Posteriormente Wikileaks, cuya cara más visible es Assange, filtró estos documentos a través de su propio sitio web haciéndolos accesibles a la opinión pública.

Estas historias ponen de relieve algunas de las paradojas que venimos describiendo. Por un lado, muestran la persistencia de los gobiernos por ejercer una vigilancia 'arriba-abajo" a través de las tecnologías de la comunicación digital y, por el otro, la creciente capacidad de individuos particulares y organizaciones ciudadanas para servirse de estas ya no solo para fiscalizar o denunciar, sino también para difundir efectivamente determinadas prácticas de esos gobiernos. Se observa, por tanto, una reciprocidad vertical manifiesta entre los procesos de vigilancia 'arriba-abajo" y 'abajo-arriba".

Bien es cierto que estos dispositivos tecnológicos que se cruzan no implican necesariamente proporcionalidad ni en cuanto a la intensidad de la vigilancia, ni en cuanto a la capacidad de alcance de unos y otros. Además, parece evidente que el control de las comunicaciones convive aún con la coerción y con la disciplina ejemplarizante del encierro. No hay que olvidar que en la actualidad el destino de estos protagonistas se ve abocado de una u otra forma a la reclusión: Manning se encuentra en prisión, mientras que Assange y Snowden están en busca y captura. Este tipo de acciones represivas contribuyen a desequilibrar la correlación de fuerzas, mediatizan el juego de la vigilancia y mandan un claro mensaje de poder. La autoridad despliega así un rótulo de advertencia para aquellos que estén tentados a entrar en este juego. Pero, por otra parte, no es menos cierto que el equilibrio de las estructuras de poder está constantemente sometido a las tensiones de las negociaciones y luchas que los distintos actores despliegan en el tablero socio-político; y es ahí, precisamente, donde la socialización de este tipo de tecnologías inaugura un contexto contingente directamente relacionado con una capacidad sin precedentes por parte de la ciudadanía para la observación, la reproducción y la difusión de prácticas gubernamentales ilícitas.

El 'juego de la vigilancia" es, en definitiva, un 'juego de poder" y de la misma forma que no puede existir democracia sin contrapoderes efectivos, una democracia no puede ser efectiva sin el derecho a ejercer la *contravigilancia*. Tradicionalmente ejercido sobre todo por el cuarto poder, la Prensa, encontramos cada vez más iniciativas

ciudadanas que reclaman este derecho y se sirven de los avances tecnológicos para ejercerlo. Como consecuencia de ello, gobiernos, empresas y estamentos de diversa índole acceden a una coyuntura que exige un reacomodo más frecuente en sus prácticas. Algunas de estas iniciativas en España son, por ejemplo, los distintos proyectos de la fundación ciudadana Civio para incentivar el libre acceso y tratamiento de los datos públicos, la labor de la Red Ciudadana Partido X y su entorno en la investigación y denuncia de la corrupción, o Filtra.la, un espacio similar a Wikileaks que también recoge denuncias por parte de ciudadanos anónimos.

Al otro lado del espejo digital

Sin embargo, pese a todo lo anterior, paralelamente a estas formas vigilantes verticales, bidireccionales, asimétricas y explícitas, se despliega un panorama de control mucho más complejo y sutil que, al ser inmanente a las tecnologías digitales que empleamos para relacionarnos, dificulta su identificación. Deleuze supo bien expresar metafóricamente lo anterior cuando, al comparar las sociedades de control con las sociedades disciplinarias, dijo aquello de que los anillos de una serpiente podían ser todavía más complicados que los agujeros de una topera.[16] Y es que no basta con constatar que el gran teleobjetivo del Gran Hermano gira intermitentemente sobre sí mismo para que podamos ver desde abajo lo que hay arriba; sino que, además, comprobamos que este se ha dispersado en un torbellino de lentes portátiles que no hacen sino relanzar el control sobre lo mundano, sobre 'el otro", sobre lo antaño privado. Estaríamos ante la sofisticación de un proceso normalizador donde la vigilancia directa da paso a un control reticular latente, una suerte de panóptico contemporáneo en el que todos pasamos a ser pequeños *Big Brothers*.[17] El *collage* de la vigilancia se ve así complicado cuando nos convertimos en un ejército de observadores móviles dispuestos en red y con potestad para controlar parcelas cada vez más amplias de lo que sucede en planos equivalentes al propio.

Más concretamente, el tándem formado por la Web 2.0 y la tecnología móvil define hoy un espacio de comunicación caracterizado por la interactividad, la ubicuidad y la inmediatez; y, de paso, habilita nuevas formas de relación con nuestra información personal y con la de los demás. Este espacio, en principio virtual, impregna de tal forma al espacio físico que son ambos los que conforman ya ese intenso escenario híbrido e hiperconectado en el cual nos relacionamos habitualmente. Convivimos con los otros combinando la red con la calle, el trabajo y el hogar. Habitamos, por tanto, un entorno fusionado donde el perfil virtual que generamos en las redes sociales de internet está

[16] G. Deleuze, *Op. cit.*
[17] L. Melgaço, *Op. cit.*

continuamente expuesto al *stalkeo*[18] y ello tiene como consecuencia la alteración de un régimen de visibilidad que resitúa la frontera entre lo público y lo privado. Un régimen que reestructura la privacidad como un asunto anguloso y contradictorio.

Vertemos continuamente información sobre nosotros mismos en la web. Buscadores, plataformas y redes sociales que usan *software privativo* recopilan datos apelando constantemente a la participación de sus usuarios, a que indiquen qué les gusta, expresen opiniones, compartan el máximo de información posible y narren sus vidas. Una suerte de *transparencia radical*, como ha dado en llamar el colectivo de investigación Ippolita.[19] Los perfiles personales de las redes comerciales se asemejan bastante a los edificios de cristal de la novela distópica de Yevgueni Zamiatin, «Nosostros», a través de cuyos muros se podía ver todo lo que la gente hacía en el interior de sus casas.[20]

Pero no se trata solo de la información que compartimos conscientemente al configurar nuestro perfil dentro del marco de posibilidades de privacidad que ofrece cada plataforma; se trata también de la *huella digital* que dejamos al navegar. Esto último significa que nuestra experiencia de navegación deja un rastro informático conformado por *cookies*, *plugins*, *pixels, direcciones Ip*… Un rastro que es analizado por agencias de datos de comportamiento y redes publicitarias mediante sistemas algorítmicos capaces de visualizar y tratar cantidades masivas de datos, lo que se conoce como *Big data*.

Al igual que ocurre con la vigilancia directa, muchas iniciativas se rebelan frente al rastreo de datos. Encontramos ejemplos tan variados como la Free Software Fundation (FSF), liderada por Richard Stallman; el sistema de navegación anónima The Onion Router (TOR), recomendado por Snowden; o TrackMeNot, una extensión inspirada en las ideas del teórico de la vigilancia Gary T. Marx que oculta el rastro de las búsquedas redirigiendo a pistas falsas.

No obstante, como ha señalado recientemente Michael Bletsas, jefe de computación del MIT Media Lab, las expectativas de privacidad heredadas del siglo XX son cada vez menos realistas.[21] La digitalización masiva de los espacios de comunicación se ha implementado de la mano de herramientas digitales

[18] *Satlker*, del inglés, acosador. El término no se aplica literalmente a las redes sociales, sino que hace referencia a revisar el perfil de otra persona, su muro de Facebook, sus comentarios, su TL de Twitter, sus fotos de Instagram…

[19] Ippolita (colectivo), *En el acuario de Facebook. El resistible ascenso del anarco-capitalismo*, En Clave de Libros, Madrid, 2012.

[20] Y. Zamiatin, *Nosotros*, Tusquets, Barcelona, 1991.

[21] E. Mallol y A. Plasencia, «Debes saber que si un servicio es gratuito el producto eres tú», *El Mundo*, 28 de noviembre de 2014, disponible en: http://www.elmundo.es/economia/2014/11/28/547772eee2704e295e8b457d.html. Acceso: 5 de diciembre de 2014.

comercializadas por la empresa privada cuyo uso proporciona una serie de ventajas tangibles y sus inconvenientes aparecen solapados. El 'ser digital" que pronosticara Nicolás Negroponte[22] parece haberse consumado en este contexto empresarial y nos encontramos ya inmersos, casi sin darnos cuenta, en una nueva fase de conectividad total.

Así las cosas, el temor a la exclusión del circuito social comunicativo actúa como fuerza magnética que atrae a la participación voluntaria de un control donde, retomando a Deleuze, el *marketing* y la publicidad se erigen como los nuevos aparatos normalizadores que complementan las viejas disciplinas.[23]

Las tecnologías que se usan en *Big data* consiguen extraer y combinar gran parte de la información que de una u otra forma proporcionamos y generan perfiles particulares basados en nuestros hábitos de navegación. Generalmente esta información es empleada con fines publicitarios; sin embargo, el caso de Snowden mostró cómo las corporaciones que explotan la web pueden compartir esa información con los gobiernos con total impunidad.

Es precisamente en esta intersección donde la vigilancia parece desprenderse de la necesidad de encierro, y lo hace en favor de un control de la comunicación que contribuye a perfilar el *marco estadístico-normalizador* que modulan las subjetividades de los usuarios de la red.[24] En las sociedades de control nuestro reflejo en las pantallas digitales podría asimilarse a un paseo por un laberinto de espejos deformantes que en función de nuestra posición nos devuelve una imagen u otra.

En todo caso, la arquitectura de ese laberinto no deja de ser un diseño fundado en las relaciones de poder que empresas, gobiernos y ciudadanos establecen entre sí. Es decir, hablamos de *una cuestión política* y, como le dijo Humpty Dumpty a Alicia, al final, lo importante es *quién manda*.[25] Es por ello que, una vez más, tomar prestada la mirada caleidoscópica de Burroughs puede ser un buen reclamo a la comprensión de este *collage* de tecnologías que nos contempla y emprender así conscientemente la responsabilidad política que implica dilucidar en qué forma queremos que lo haga.

Who Controls Control The Men	*Controls Who The Men Control*	*Control Who Men The Controls*
Who Controls Men The Control	*Controls Who Control Men The*	*Control Controls The Men Who*
Who Controls Men Control The	*Controls Who Control The Men*	*Control Controls The Who Men*

[22] N. Negroponte, *Being Digital*, Vintage USA, Random House, 1995.
[23] G. Deleuze, *Op. cit.*
[24] Véase A. Segura, «El pastor, el doctor y el Big Data», *Revista Teknokultura*, Vol. 11, n° 2, pp. 243-257.
[25] En L. Carroll, *A través del espejo y lo que Alicia encontró al otro lado*, Alianza, Madrid, 2005.

Hacia un urbanismo *securitario*. El mantenimiento del orden en el espacio y a través del espacio

Jean-Pierre Garnier
Sociólogo urbano

Traducción de María Castrillo revisada por el autor[*]

Más vale prevenir que curar, dice el refrán. Y este principio está siendo aplicado al pie de la letra por los gobernantes de nuestras sociedades, donde la precarización, la pauperización y la marginalización de masas están haciendo salir a la calle a quienes les ha tocado pagar el pato, unos para protestar y reivindicar, otros para cometer actos de 'violencia urbana" o incluso hechos de carácter delictivo. Se habla entonces convencionalmente de 'alteraciones del orden público" y, como los gobiernos no pueden curar los males sociales que son las desigualdades crecientes, el paro y la miseria producidos por un orden cuya naturaleza 'democrática" pretenden incontestable, en vez de dirigirse contra la verdadera causa de esas 'alteraciones" simplemente se dirigen contra sus autores.

Su objetivo, pues, no es resolver la cuestión social sino *regular* los efectos de su no-solución. El contexto socioeconómico y político-ideológico general es obviado e incluso se procura no mencionarlo para evitar que parezca una 'excusa sociológica" inspirada por un cierto 'angelismo", y todo ello simplemente en beneficio de las circunstancias inmediatas y locales que son supuestamente el origen de los actos y de las conductas reprobables o pretendidas como tales. Se hace alusión, además, a un sinfín de *riesgos*, desde el terrorismo a toda una lista que no deja de ampliarse y que corre en paralelo a la de las categorías de malhechores asociadas: robo, estafa, agresión, vandalismo, tráfico de droga, mendicidad, prostitución, vagabundeo de los sin techo o sin papeles, reuniones tumultuosas, motines y, por supuesto, manifestaciones –autorizadas o no–, entre otras innumerables 'incivilidades".

Este tratamiento de los desórdenes urbanos sin curación posible toma tres vías alternativas o complementarias. La primera, la más clásica, es la mera represión con el uso pretendidamente legítimo de la fuerza física, cuyo monopolio no solo está detentado por el Estado sino que además, según el sociólogo Max Weber, define a este.

[*] María Castrillo es docente del Instituto Universitario de Urbanística y profesora titular de Urbanística y ordenación del territorio de la Universidad de Valladolid.

Una segunda vía, denominada prevención social, tiende a *insertar* a los individuos o grupos 'de riesgo" con ayuda de medidas que se suponen influyen de manera positiva sobre su personalidad, mejorando eventualmente sus condiciones de vida (empleo, escolaridad, vivienda, cultura, distracción), mientras dejan intactas las relaciones de dominación y de explotación que están en el origen de ellas. Una tercera vía, intermediaria entre las dos anteriores, bautizada como prevención situacional, consiste en anticipar, por medio de dispositivos de vigilancia, control y protección, situaciones propicias al acometimiento de infracciones o de actos oficialmente clasificados como alteraciones de la paz civil[26] o incluso como terroristas, convirtiéndolas en más difíciles, más arriesgadas o menos ventajosas para sus autores (reales, supuestos o potenciales). Es aquí donde entran en juego los urbanistas y los arquitectos para hacer que el espacio urbanizado sea *defendible.*[27]

En efecto, aplicada al espacio urbano, la prevención situacional consiste en reconfigurarlo físicamente con objeto de disuadir de malas intenciones a los individuos, aislados o en grupo, y, en caso de que pasasen a los actos, de facilitar la intervención de las 'fuerzas del orden". En otras palabras, se trata de una estrategia del mantenimiento del orden en el espacio y a través del espacio que combina dos elementos: impedir que ocurran hechos delictivos o considerados como tales, y permitir a la policía o incluso al ejército una mayor eficacia en la represión.

A grandes rasgos, las orientaciones de esta estrategia han sido esbozadas por tres especialistas en arquitectura y urbanismo anglófonos. Primero, la filósofa Jane Jacobs, que propondrá «la *securización* del espacio de la ciudades a través de la animación urbana».[28] Su hipótesis de partida es que la *vigilancia natural* de los espacios comunes que están al alcance de la vista de los propios habitantes –se trata en realidad de una vigilancia más o menos espontánea socialmente acondicionada– contribuye a impedir los actos de malevolencia. Esto implica que el reordenamiento urbanístico y arquitectónico debe producir formas espaciales capaces de hacer que cada quien pueda 'ver y ser visto". Sin embargo, será el arquitecto-urbanista estadounidense Oscar Newman quien ponga en órbita (ideológicamente hablando) el pseudo-concepto de *espacio defensivo* (*defensive space*).[29] *Su tesis, cercana a la de Jacobs, es que la inseguridad urbana se debe a una falta de control visual, por parte de los ciudadanos, de su medio ambiente. De ahí se desprende que el espacio debe ser reorganizado teniendo como base las solidaridades vecinales y una clara delimitación de los tipos de ocupación del espacio que, debidamente jerarquizados en privados,*

[26] Paz civil: neologismo eufemizante con que se designa en Francia al 'orden público". Tiene claras vinculaciones con la pacífica conviviencia en el sentido jurídico con que se emplea en España.
[27] J.P. Garnier, «Un espacio indefendible. La reordenación urbana en la hora *securitaria*», en *Contra los territorios del poder. Por un espacio publico de debates... y de combates*, *Virus, 2006* (disponible en descarga directa desde la web de la editorial).
[28] J. Jacobs, *Muerte y vida de las grandes ciudades*, Capitán Swing Libros, 2011.
[29] O. Newman, *Defensible space. Crime prevention through urban design*, MacMillan, 1972.

semiprivados y públicos, propiciarían una disminución de las zonas de conflicto. La tercera inspiradora remodelación securitaria del espacio urbano es la de la geógrafa inglesa Alice Coleman, para quien existiría un vínculo entre el aumento de la criminalidad y la construcción en serie de «edificios gigantescos y anónimos de viviendas sociales» donde «se amontonan las familias» conforme, según ella, a «la utopía socialista» del Movimiento moderno en arquitectura, ese que «negaba con arrogancia el deseo innato de la gente de tener su propio espacio privado, preferentemente con un jardín». [30] La solución, para Coleman, era la regeneración urbana, es decir, la destrucción o el fraccionamiento de los grandes edificios en provecho de pequeños conjuntos de viviendas, cada uno de ellos con una área verde semiprivada.

Como se puede observar, estos análisis y preconizaciones están inspiradas en un enfoque *espacialista* de la realidad social, esto es, se basan en el postulado de una cierta capacidad de determinación de los comportamientos a través el entorno construido. Según esta ideología, el espacio puede ser tanto la causa como el remedio de algunos males sociales. Así, por ejemplo, la degradación de las condiciones materiales de habitación en los polígonos de vivienda social explicaría en gran parte la degradación moral que atestiguan los actos y actitudes de algunos de sus habitantes. De hecho, en este sentido, se hablará de 'espacios criminógenos" y, como consecuencia, de la necesidad de operaciones de 'regeneración urbana". A nadie sorprenderá que estas teorías y los modelos urbanísticos que han inspirado procedan de adeptos a la economía de mercado o, con otras palabras, al neoliberalismo. Para ellos y para las autoridades a las que asesoran, si hace falta cambiar la ciudad solo es para evitar que cambie la sociedad. ¡No es casualidad que Margaret Thatcher considerase a Alice Coleman su arquitecta favorita! [31]

El urbanismo *securitario* fue importado en Francia bajo el nombre de «arquitectura de prevención situacional» en el marco de una Ley de Orientación y de Programación para la Seguridad (LOPS), aprobada en 1995. En los años que siguieron, y siempre para responder a «una demanda creciente de seguridad del espacio público», este modelo ha sido completado y reforzado sin cesar por otras leyes o reglamentaciones, todas ellas dictadas en el marco 'democrático" de la alternancia en el poder de la verdadera derecha y la falsa izquierda. Como es costumbre entre los gobiernos franceses, los cambios de denominación buscan disimular con palabras los objetivos realmente perseguidos. Así como la noción de *espacio defensivo* haría demasiado evidente que ciertas remodelaciones espaciales estarían respondiendo a un imperativo de defensa 'social", el lema oficial que orientará la intervención de los planificadores urbanos franceses evitará toda sombra de sospecha: «ordenar los

[30] A. Coleman, *Utopy on trial: Vision and reality in planned housing*, Hilary Shipman, 1985.
[31] L. Hunter-Tilney, "Architecture: Paradise lost", entrevista con A. Coleman. *New Statesman*, 12 de marzo de 2012.

lugares para prevenir el crimen». Desde el Ministerio del Interior y las instituciones estatales a las que compete el ordenamiento del espacio urbano hasta las prefecturas, ayuntamientos, organismos de la vivienda social y empresas de promoción inmobiliaria y también en los institutos de urbanismo y escuelas de arquitectura se ha propalado así la idea de que la forma de los edificios y de los espacios públicos podría, según los casos, ayudar o estorbar los manejos de los eventuales perturbadores y las acciones de represión policial.

De este modo, arquitectos y urbanistas, pero también paisajistas y diseñadores, a los cuales se añade toda una cohorte de sociólogos, geógrafos y antropólogos urbanos que hacen suya la finalidad policiaca de la 'gobernanza" de las ciudades, prestan su ayuda a las autoridades para la preservación de la 'tranquilidad pública" en los territorios urbanizados. Además de la proliferación de las cámaras de videovigilancia y de los controles electrónicos de acceso a los edificios, cada vez más artefactos múltiples con finalidad securitaria se integran en los planes urbanísticos y en los proyectos arquitectónicos: urbanizaciones cerradas, *residencialización* de los bloques de vivienda social (privatización de los espacios libres comunes exteriores), supresión de los lugares-trampa –callejones sin salida, pasajes oscuros, muretes, rincones, cubiertas planas, pasarelas, corredores, vestíbulos con doble entrada, etc.–, instalación de mobiliario urbano disuasorio –bolardos contra 'alunizajes" o similares,[32] bancos anti-mendigos–, eliminación de los obstáculos visuales en los espacios públicos y distribución de los edificios residenciales de forma que permitan la llamada *vigilancia natural* por parte de los vecinos o transeúntes, vegetalización disuasiva –setos 'anti-atraco" a lo largo de las fachadas, a veces con espinas venenosas–, supresión del aparcamiento al pie de los edificios y de las escaleras entre de los bloques de viviendas sociales para facilitar los desplazamientos de las motos, coches y camiones de la policía e incluso los blindados del ejército. Todos estos elementos y otros muchos se conjugan entre sí con vistas a un solo fin: incitar a los 'delincuentes" y 'subversivos", reales o potenciales, a dejar de considerarse los 'dueños del terreno".

Sin embargo, en Francia como en otras partes, estos dispositivos espaciales han sido criticados, no solamente por los adversarios del neoliberalismo y los militantes anticapitalistas, sino a veces también por algunos defensores del orden establecido, ya sean policías, investigadores en ciencias sociales o arquitectos, que los juzgan como contraproducentes, ineficientes y antiestéticos. Según ellos, dan lugar a una ciudad bunkerizada, panóptica** y paranoide compuesta por enclaves cerrados replegados

[32] En francés *voitures-béliers*, coches utilizados para romper cajeros automáticos.

** El panóptico es un tipo de arquitectura carcelaria ideada por el filósofo utilitarista Jeremy Bentham hacia fines del siglo XVIII. El objetivo de la estructura panóptica es permitir a su guardián, guarnecido en una torre central, observar a todos los prisioneros, recluidos en celdas individuales alrededor de la torre, sin que estos puedan saber si son observados. El efecto más importante del panóptico es inducir en el detenido un estado consciente y permanente de visibilidad que garantiza el funcionamiento automático

sobre sí mismos para proteger a sus habitantes o sus usuarios legítimos contra los 'extraños", vistos, por ello mismo, como sospechosos e incluso indeseables. Esa crítica interna securitaria no vacilará en hablar de 'ecología del miedo" –retomando la fórmula del antropólogo urbano radical Mike Davis–[33] ni en denunciar el efecto a veces angustioso que producen sobre la población esos entornos *securizados* que parecen inquietarla más que tranquilizarla.

Obviamente, la necesidad de 'defender la ciudad" –como ya dije, se trata en realidad de defender el orden social capitalista que se impone a esta– nunca ha estado menos puesta en tela de juicio que ahora,[34] cuando el 'enemigo" está tanto más presente cuanto es cada vez menos definible: a la vez exterior e interior, local y global, real y virtual. Para los estrategas más innovadores de la 'pacificación urbana", es preciso establecer un nuevo modelo de organización y de funcionamiento del espacio urbano, más sofisticado y más sutil. En realidad, lo uno no contradice lo otro y ambos van a combinarse. A la ciudad-fortaleza descrita y denunciada por Mike Davis, en la que se prohíbe o limita la entrada a ciertos lugares de perturbadores reales o potenciales, se superpone ahora la «regulación de los flujos por medio de la separación de las circulaciones por tipos de públicos, de tal manera que se eliminen los riesgos de fricción social y humana».[35] Así, la protección física de ciertos espacios irá de ahora en adelante a la par con la gestión de los desplazamientos.

Hoy día se trata además de constituir un espacio adaptable a cualquier situación, incluso las que ya no puede controlar la propia sociedad compleja que las genera, una sociedad 'movediza" que obliga a los ciudadanos a moverse en la incertidumbre y que, según la metáfora del sociólogo Zygmunt Bauman, se habría vuelto *líquida*.[36] Haciéndose eco de politiqueros, periodistas y expertos *mainstream,*[37] el arquitecto Paul Landauer apunta que, «desde las incivilidades al terrorismo, pasando por las agresiones y las violencias urbanas», la delincuencia estaría asimismo conformándose a imagen de la sociedad: «cada vez más movediza y volátil».[38] Así que ya sería hora de anticipar lo imprevisible, de enfocar lo improbable. Todo puede ocurrir en cualquier lugar y en cualquier momento. Se habla a este respecto de la necesidad de una 'gobernanza de lo aleatorio". «Frente a una inseguridad plural y movediza, la seguridad no puede ser sino global y evolutiva», dicen los autores de un libro de recetas

---

del poder, sin que ese poder se esté ejerciendo de manera efectiva en cada momento, puesto que el prisionero no puede saber cuándo se le vigila y cuándo no. Fuente: Wikipedia. N. del E.

[33] M. Davis, *Contrôle urbain, écologie de la peur*, Ab Irato, 1997.
[34] Th. Oblet, *Défendre la ville. La police, la ville et les habitants*, PUF, col. La ville en débat, 2008.
[35] P. Landauer, *L'architecte, la ville et la sécurité*, PUF, 2009.
[36] Z. Bauman, *Le présent liquide. Peurs sociales et obsessions sécuritaires*, Le Seuil, 2007.
[37] M. Rigouste, *Les marchands de peur*, Libertalia, 2010.
[38] P. Landauer, *Op.cit.*

dirigido a arquitectos, urbanistas y paisajistas para ayudarles a «apropriarse del campo de la seguridad».[39]

Igual que la inseguridad ya no sería de antemano exclusiva de las 'clases peligrosas" –la clase obrera, en particular–, tampoco sería ya propia de lugares específicos, «de calles desiertas y de barrios 'calientes"» (aunque las zonas de relegación llamadas 'barrios vulnerables", donde está confinada una parte de las clases populares, siguen siendo las primeras en las prioridades de regeneración con el objetivo de 'pacificarlas"). Ahora se entiende que los espacios urbanos más 'expuestos" son los más frecuentados por gentes de toda índole: infraestructuras de transporte, centros comerciales, equipamientos de ocio, plazas del centro de la ciudad, etc. De ahí que el urbanismo *securitario* clásico ya no baste. Además de haberse diversificado, «las poblaciones que deben ser controladas se presentan como indistintas y, al tiempo, móviles», lo que obliga a echar mano de un «urbanismo 'inteligente" –tal como se habla de tecnología 'inteligente"– capaz de modificar sus planes conforme a las circunstancias».[40]

¿En qué consiste concretamente esa 'inteligencia"? En establecer dispositivos de separación y canalización de los diferentes públicos, en limitar los cruces para evitar los embotellamientos y la congestión propicios a toda clase de actos de malevolencia –desde las raterías hasta los atentados pasando por los motines, y también en instalar 'perímetros de seguridad" móviles y extensibles que sirvan para filtrar a los usuarios según la legitimidad que se les reconozca para estar presentes en los lugares que se pretenden *securizar* o en su entorno inmediato, todo ello sin olvidar la vías especiales reservadas para las intervenciones rápidas de la policía. Estas técnicas están siendo difundidas poco a poco por todas partes en nuestras ciudades, sea cual sea el nivel de riesgo que se les suponga, en virtud de una creciente obsesión por las concentraciones imprevistas, los movimientos de la muchedumbre, las reuniones tumultuosas y los desbordamientos incontrolados. El objetivo básico es incitar al desplazamiento y disuadir del estacionamiento en el espacio público. Las palabras clave son fluidez y movilidad. La inmovilidad se convierte en sospechosa de bloquear, intencionalmente o no, los flujos. El aeropuerto y sus alrededores o el estadio de fútbol y sus inmediaciones se han convertido en el modelo para todo esto, lo mismo para desbaratar las acciones de los *hooligans* que los atentados terroristas.

Con todo, según los promotores y adeptos de un urbanismo *securitario* más *soft*, es decir más atento a «conciliar seguridad y urbanidad»,[41] aquel modelo también podría resultar excesivo y, a su vez, contraproducente. Aunque «la coacción espacial es mucho más tolerada que la represión policial», apunta el sociólogo Thierry Oblet, para

[39] *Guide des études de sûreté et de sécurité publiques*, La Documentation française, 2007.
[40] P. Landauer, *Op.cit.*
[41] *Ibid.*

que consiga sus plenos efectos, hace falta que sea discreta y no dar a los ciudadanos la nefasta impresión de vivir en un ambiente urbano carcelario. De ahí que arquitectos, urbanistas y paisajistas sean invitados a rivalizar en creatividad artística para hacer acogedores los espacios que *securizan*. Esta es la 'buena nueva" para todos aquellos al acecho de innovaciones *securitarias* en el ámbito urbano.

Sin embargo, por perfeccionados que estén, estos subterfugios estéticos no pueden superar la contradicción a la que se enfrentan los expertos en manipulaciones espaciales que, bajo la presión de sus comitentes públicos –en particular los ayuntamientos–, se desloman para hacer rimar seguridad y sociabilidad. Por eficaces que sean en términos de pacificación de conflictos y enfrentamientos urbanos, las estrategias fundadas en la separación de usuarios y en la especialización de usos –comercio, deporte, arte, fiesta…– no pueden ir en la dirección de la 'consolidación de los lazos sociales", objetivo unánime y consensual ritualmente evocado en los discursos de quienes deciden las políticas urbanas y en la prosa de sus siervos investigadores.

Ignorando deliberadamente la división de la sociedad –y, por tanto, de la ciudad– en clases, así como las desigualdades patentes y los antagonismos que genera, los que hablan de una ciudad 'ciudadana, donde cada uno contribuiría a la seguridad de todos, también cantan alabanzas a un espacio público apto para «dar lugar al encuentro entre seres libres e iguales»,[42] al tiempo que lamentan que las estrategias que dan prioridad al mantenimiento del orden en detrimento del 'vivir juntos" vayan en contra de la «preservación de un espacio común entre los hombres […] necesaria a la propia seguridad, pues solo ella puede garantizar un reparto y una distancia justa entre usuarios, habitantes, ciudadanos y visitantes».[43] De ahí, una serie de preguntas tontas elevadas al rango de problemáticas científicas: «¿Cómo provocar el encuentro en ciudades concebidas para evitar que la gente se cruce? ¿Existe una manera posible de compartir colectivamente lugares jerarquizados conforme al grado de conocimiento mutuo –donde el desconocido es percibido como un intruso o, peor, un sospechoso– y de identidad?».[44] La respuesta que se da está a la altura, si es que se puede decir así, de las cuestiones planteadas: habría que aprovechar «la consideración de la seguridad en los proyectos urbanísticos y arquitectónicos» para «encontrar la distancia justa entre los distintos miembros de la colectividad urbana, por muy diferentes que sean. Ni demasiado cerca ni demasiado lejos, ni demasiado separados ni demasiado juntos, ni demasiado en movimiento, ni demasiado inmóviles». En pocas palabras, como la distancia social se postula como intangible, la distancia espacial debe servir como variable de ajuste. ¡No tienen poco trabajo los arquitectos y urbanistas si tienen que

[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.* Con el término identidad el autor se refiere a la identidad social y racial.

demostrar que, a través de la 'distancia justa", pueden resolver los problemas de seguridad!

El Estado vigilante:
Los archivos de la NSA y la respuesta global

Ben Hayes
Investigador del Transnational Institute y de Statewatch

Traducción: Nuria del Viso[*]

> «[I]ncluso si no estás haciendo nada malo, te están observando y grabando. Y la capacidad de almacenamiento de estos sistemas aumenta cada año de forma continuada en varios órdenes de magnitud,[45] y está llegando al punto en que no hace falta que hayas hecho nada malo. Simplemente tienes que resultarle a alguien sospechoso, incluso por una llamada inapropiada. Y entonces pueden usar este sistema para retroceder en el tiempo e investigar cada decisión que has tomado, cada amigo con quien has debatido algo alguna vez. Y esto sirve para atacarte, para crear sospecha sobre una vida inocente y pintar a cualquiera como malhechor…».
>
> Edward Snowden, junio 2013

El Estado vigilante al desnudo

Si alguien nos ha dicho algo relevante sobre el poder del Estado en 2013 fue Edward Snowden, que reveló cómo la capacidad de vigilancia de algunos gobiernos democráticos occidentales son de tal magnitud que pueden acceder prácticamente a todo lo que sus ciudadanos hacen *on line* o con un teléfono móvil o fijo, en ausencia de controles democráticos o judiciales significativos.

Estos poderes están especialmente avanzados en la alianza *Five Eyes* [Cinco ojos], liderada por EEUU-Reino Unido (y que también incluye a Australia, Canadá y Nueva Zelanda), pero se sabe o se sospecha que muchos otros países europeos y de la OTAN disponen de estructuras de vigilancia avanzadas y han cooperado estrechamente con la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) de EEUU y la Sede de Comunicaciones del Gobierno del Reino Unido (GCHQ, por sus siglas en inglés). Con una industria global de vigilancia en expansión dispuesta a ayudarles, es simplemente

[*] Publicado originalmente en *State of Power 2014*, Transnational Institute (TNI), 2014. Publicado con permiso de TNI.
[45] La expresión órdenes de magnitud (by *orders of magnitude*) se refiere a la multiplicación de un número dado por 10 (N. de la T.).

inconcebible que gobiernos mucho menos democráticos no estén implicados en las mismas prácticas.

No es noticia que los espías espían, o que los poderosos utilizan la vigilancia y la subversión para mantener su poder y su ventaja comparativa. En este sentido, que EEUU-Reino Unido 'pincharan" las llamadas telefónicas de destacados políticos es una especie de atracción secundaria conveniente (la historia real es la facilidad con la que lo hicieron); lo que es nuevo e importante del estado del poder es la simplicidad con la que determinados individuos y poblaciones enteras pueden ser puestas bajo vigilancia, el papel crucial que desempeñan las empresas privadas para facilitar esa vigilancia y la ausencia de poder y autonomía que como sujetos tenemos para decidir cómo nos gobernamos y qué ocurre con la información sobre nosotros.

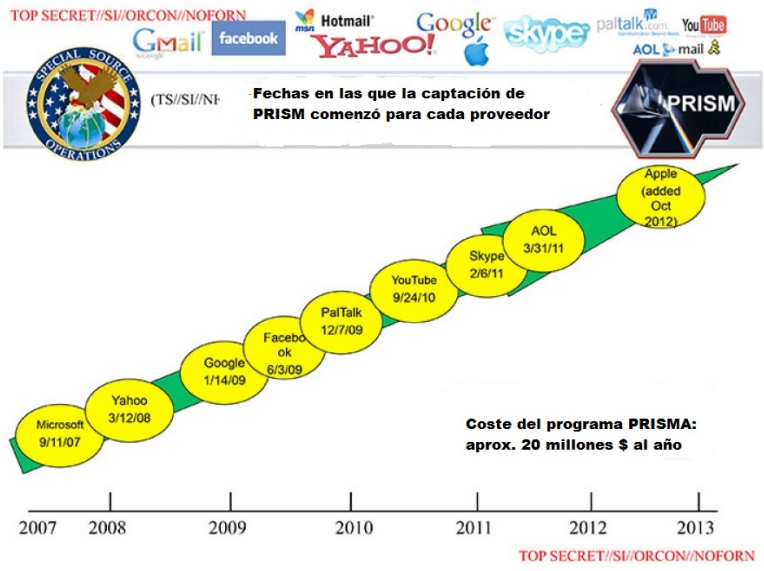
En respuesta a las revelaciones, los directores de prensa y los que destaparon el asunto de los gobiernos se han unido a más de 300 ONG y 500 destacados autores de todo el mundo para pedir un punto final a la vigilancia masiva e indiscriminada; también está circulando una declaración de Académicos contra la Vigilancia Masiva. Campañas nacionales ya con historia contra la vigilancia han rejuvenecido con las revelaciones de Snowden y un grupo de Parlamentos y organizaciones intergubernamentales están concediendo atención al asunto por primera vez. Pero de ninguna manera estas campañas en alza son garantía de una reforma significativa. Este artículo examina algunos de los principales debates en torno a la reforma sobre la vigilancia y las batallas que nos aguardan.

Revelaciones clave

Una mínima fracción de los documentos secretos liberados por Edward Snowden ha sido publicada o ha sido mencionada por los periodistas. Mientras que a Glenn Greenwald y sus compañeros se les ha acusado de todo tipo de delitos, desde apoyar a terroristas y pedófilos a traficar y esconder información peligrosa, ellos han sido tanto sensatos como responsables en la forma en que han revelado la información. Además, las noticias con cuentagotas que revelan la complicidad de un grupo cada vez mayor de empresas y países han garantizado que una de las historias de libertades civiles más importantes de los últimos tiempos ha ocupado la primera plana de los medios de comunicación en todo el mundo durante más de seis meses. Ninguna otra filtración en la historia ha alcanzado esta hazaña. Los 'momentos culminantes" de los archivos de la NSA desvelados hasta ahora incluyen:

- La orden judicial *Verizon*: el primero de los filtrajes de Snowden reveló que la NSA guardaba las grabaciones telefónicas de millones de americanos. Aunque la iniciativa fue lanzada por la administración Bush, mucha gente creía que Obama la había suprimido.

- Programa PRISM: permite a la NSA y al GCHQ 'recabar" información de los servidores de algunas de las mayores empresas tecnológicas de EEUU (Google, Apple, Microsoft, Facebook, AOL, PalTalk y Yahoo). Un programa similar llamado Muscular interceptaba millones de registros al día de Yahoo y Google.
- Tempora, parte del programa Mastering the Internet: el GCHQ intercepta y almacena la mayor parte de los datos que entran y salen del Reino Unido a través de los cables de fibra óptica submarina, que son las venas de la World Wide Web. Programas similares de 'interceptar a bulto" gestionados por la NSA (Blarney, Fairview, Oaksatar y Stormbrew).
- Xkeyscore: un sistema de recuperación de datos utilizado por la NSA y usado para acceder a emails, llamadas telefónicas, registros de uso de internet y documentos transmitidos en internet.
- Boundless informant: un sistema de análisis y visualización de datos que proporciona una visión de conjunto de las actividades de vigilancia de la NSA por país o programa. Casi 3.000 millones de 'unidades de datos" del interior de EEUU fueron capturados por la NSA durante un periodo de 30 días en marzo de 2013, según informaciones.
- Bullrun y Edgehill: un programa de 250 millones de dólares al año bajo el que la NSA y la GCHQ (respectivamente) rompieron la mayor parte dela tecnología deencriptación, que es la base de la seguridad de internet.
- Ciberguerra, espionaje y conspiración: revelaciones posteriores han detallado hasta qué punto EEUU está preparado para utilizar ciberataques internacionalmente «para impulsar los objetivos de EEUU en todo el mundo», el seguimiento de llamadas telefónicas a 35 líderes mundiales y la complicidad en la vigilancia NSA-GCHQ de los servicios de inteligencia de, entre otros, Bélgica, Dinamarca, Francia, Alemania, Italia, Japón, Holanda, Noruega, Singapur, Corea del Sur, España y Suecia.



Fuente: Diapositivas de la NSA, *The Washington Post*, junio de 2013

«A través de cualquier medio»

Como Snowden explicó desde el principio, este despliegue desconcertante de programas secretos de vigilancia demuestra la dimensión a la que la 'comunidad de inteligencia" llegará para «obtener información donde pueda y por cualquier medio posible».

Se están vigilando redes completas de comunicación, ya sea 'legalmente" (en el sentido de que el acceso a los datos que transportan es requisito legal sancionado por orden judicial que ofrece una ámbito de actuación sin límites), bajo acuerdos de cooperación 'voluntarios" (entre las agencias de inteligencia y las empresas propietarias de estas redes) o a través de 'pinchazos" promovidos por los estados (interceptación de cables de fibra óptica y centros de datos que albergan esas redes).

La NSA también ha estado creando 'puertas traseras" en las aplicaciones y software de algunas de las mayores compañías TIC del mundo y utilizando software malicioso para robar información de redes privadas, gubernamentales y empresariales. Existe un documento que sugería que la NSA ha 'infectado" más de 50.000 redes de ordenadores en todo el mundo.

Juntos, la NSA y la GCHQ han puesto en peligro la criptografía que permite la transmisión segura de información a través de la mayor parte de internet. Tim Berners-Lee, inventor de la World Wide Web, calificó sus maniobras de «abominables y estúpidas» porque «beneficiarían a los grupos criminales de hackers y a los estados hostiles», y añadió que él estaba «muy de acuerdo con los intentos de aumentar la seguridad contra el crimen organizado, pero te tienes que distinguir del criminal».

A menos que creas que las actividades reseñadas más arriba son actos totalmente apropiados para los gobiernos democráticos, las acciones de Edward Snowden son la encarnación de la actuación con principios para destapar la olla y le debemos enorme gratitud. El hecho de que se ha visto forzado a pedir asilo en Rusia, no solo de EEUU, sino de los socios europeos, algunos de los cuales mostraron un desprecio sin precedentes por las convenciones diplomáticas al obligar a aterrizar el avión del Presidente de Bolivia para buscar a Snowden, deshonra a todos los involucrados y dice mucho de los valores y los intereses de los actuales gobiernos occidentales.

Grandes bases de datos, mayores problemas

Al considerar cómo la vigilancia encaja en el actual estado del poder, que ha cambiado completamente desde los tiempos en que la Stasi tuviera a poblaciones enteras fichadas, es que infraestructuras privadas se ha convertido en la primera línea de la

recopilación de información. A su vez, la vigilancia masiva de la población ya no es solo el elemento que preserva a los regímenes totalitarios, sino un elemento básico de países democráticos.

La revolución en las tecnologías de la información y las comunicaciones (TIC) está transformando nuestras relaciones con todos y con todo. A medida que más y más de nuestras relaciones se desarrollan *on line* –las interacciones con amigos y conocidos se producen a través de las redes sociales; con empresas y proveedores de servicios a través del comercio electrónico; con bancos y con servicios electrónicos de la administración y con campañas políticas–, se recopila más y más información sobre nosotros. Todo se graba, almacena y analiza, mientras que cada año se fortalecen los argumentos económicos y organizativos para guardar esos datos eternamente.

Lo que hacemos en el mundo digital traiciona nuestros pensamientos, intereses, hábitos, atributos y características. Y como especie se pone de manifiesto que somos totalmente predecibles: 'embarazosamente", según un ex consejero general de la NSA. A medida que más y más de las cosas que poseemos están conectadas al mundo digital y utilizamos más y más servicios *on line*, producimos más información sensitiva y completa: dónde estuvimos, qué hicimos y con quién.

Dejamos estos datos por todas partes. Incluye datos personales (información que nos identifica), de contenido (lo que escribimos y decimos) y 'metadatos" (datos sobre datos, como registros de llamadas, tráfico de internet, datos de localización, etc.). Muchas innovaciones digitales se basan en la recogida y análisis de esta información, desde los mapas en nuestros *smart phones* a las numerosas aplicaciones a través de las cuales se comparte y consume la información y la cultura. La necesidad de protegernos de las agencias de inteligencia y seguridad, empeñadas en sortear nuestro derecho a la privacidad, constituye solo una parte del problema. También necesitamos saber que estamos protegidos de esas compañías, cuyo balance depende de acceder (y mercantilizar) cuanta información personal sobre nosotros les sea posible.

Ambos problemas se agudizan por un tercero: los '*big data*", o grandes bases de datos, que es menos un concepto que un lema del *marketing* para encapsular una nueva industria. «¿Tiene una gran base de datos? Le ayudamos a entender a sus clientes, usuarios, empleados, redes, amenazas, riesgos, oportunidades, etc.». Aquí es donde la 'cara oculta" de las TIC –lo que Naomi Klein describió atinadamente como la «fusión entre el centro comercial y la prisión secreta»– se muestra sin tapujos. Los mismos algoritmos y herramientas de análisis que usa Facebook para entender tus intereses y deseos, y que Amazon utiliza para calcular (y calcular erróneamente) qué más puedes querer comprar, pueden ser utilizados por gobiernos y compañías de seguridad privadas para calcular (y calcular erróneamente) si puedes ser una amenaza, ahora o en el futuro. Y es precisamente la naturaleza de 'doble uso" de esta tecnología

lo que la hace tan difícil de regular. «No es un sistema de vigilancia, es un conjunto analítico de datos», es el discurso en el que se basa este pujante comercio internacional en un formato verdaderamente orwelliano.

Cuestionar las redes de vigilancia que desveló Edward Snowden es relativamente sencillo: se trata de agencias de inteligencia y seguridad que actúan sin freno en una infraestructura digital insegura y utilizan poderes fuera de control heredados de la era analógica, parafraseando a Human Rights Watch. Lograr reformas de relevancia que aborden adecuadamente este problema es mucho más difícil en virtud de los intereses que existen para mantener el *status quo* y los problemas jurisdiccionales que surgen frente a cualquier intento de restricción de las redes de vigilancia transnacionales. Estas cuestiones remiten a cambios profundos en las relaciones entre la ciudadanía, los Estados y las corporaciones.

¿Silicon Valley vs NSA?

En diciembre de 2013 ocho de las firmas tecnológicas de más éxito de Silicon Valley –Aol, Apple, Facebook, Google, Linkedin, Microsoft, Twitter y Yahoo– hicieron un llamamiento a favor de «cambios a gran escala» de la vigilancia del Gobierno de EEUU basado en cinco principios de reforma: i) 'límites razonables" a la recogida de información del Gobierno y el fin de la 'captura masiva de datos"; ii) mayor control y rendición de cuentas de las agencias de inteligencia; iii) transparencia sobre las demandas del gobierno y poderes de vigilancia; iv) respeto al 'libre flujo de información" y v) un 'marco robusto, transparente y basado en principios" para regular peticiones lícitas de datos a través de las jurisdicciones.

Esta iniciativa se basa en pasos tentativos anteriores a favor de una mayor transparencia en la vigilancia en virtud de la cual algunas de estas compañías han publicado información comparativa sobre las demandas del Gobierno y autoridades competentes de los datos de sus usuarios, mientras pedían al Gobierno de EEUU que les permitiera publicar información de los –hasta entonces– tratos secretos con la NSA. Es de destacar que las compañías de telefonía fija y móvil, muchas de las cuales han estado facilitando información al Estado sin cuestionarlo durante mucho más tiempo que sus contrapartes de internet, no han intervenido en el debate de la misma manera; aunque tampoco se pronunciaron nunca a favor de la democracia.

Dice mucho sobre el estado del poder el hecho de que lo que preocupara y moviera a la acción a la Casa Blanca fuera que las revelaciones pudieran perjudicar especialmente a algunas de las corporaciones más poderosas de EEUU. Pero también plantea cuestiones más generales sobre cómo se ejerce el poder corporativo. Algunas de estas compañías han colaborado (en muy distintos niveles) en la vigilancia estatal, pero algunas también han resistido ferozmente la tentativa de una legislación

diseñada para dar a los individuos mayor control el destino de sus los datos personales, datos de los que dependen los márgenes de beneficio de tales corporaciones, incluidas las aportaciones al borrador de la UE sobre Regulación de la Protección de Datos.

«Te ayudaremos a protegerte de la vigilancia gubernamental, pero no hace falta que te protejas de nosotros» es una propuesta para un grupo de compañías que, según *Forbes*, destinaron más de 35 millones de dólares a actividades de *lobby* el año pasado. Google absorbió la mitad del total (18,2 millones de dólares); si se excluyen las asociaciones patronales y grupos de presión, solo General Electric admite gastar más en *lobby* (Microsoft, 8,1 millones de dólares; Facebook, 3,9 millones; Yahoo; 2,8 millones y Apple, 2 millones, conforman casi la totalidad del resto hasta el total de 35 millones).

No cabe duda de que estas compañías se oponen sinceramente a la vigilancia y almacenamiento de datos masivo que lleva a cabo la NSA porque es un riesgo genuino al espíritu de su negocio. Como indica el Consejo General de Microsoft, «la gente no utilizará tecnología de la que no se fía. Los gobiernos han puesto en riesgo esa confianza y los gobiernos tienen que restaurarla». Pero al mismo tiempo que sus máximos dirigentes se dirigen a Davos para demandar más transparencia y control de la vigilancia para preservar la 'integridad de internet", debemos preguntarnos qué más buscan y reciben de nuestros líderes y legisladores. También debemos preguntar al sector tecnológico europeo dónde se sitúan respecto a la reforma en la vigilancia y por qué no ha asumido sus responsabilidades.

¿Europa vs el 'Gran Satán"?

La indignación pública ante las revelaciones de Snowden es tal que actualmente hay capital político significativo vinculado a la reforma de la vigilancia. Pero lo que se han considerado críticas y demandas de cambio procedentes de Angela Merkel y Barack Obama no han ido paralelas, al menos hasta ahora, con la acción política. Ciertamente, a pesar de las reformas cosméticas, existe poca evidencia de que haya verdadera voluntad de cambios estructurales más profundos tan notoriamente necesarios.

Los gobiernos de la UE aprobaron una declaración conjunta de crítica a su socio transatlántico y avisando de un derrumbe de la confianza, pero no han anunciado ninguna sanción. Los gobiernos europeos, que han expresado abiertamente sus críticas a las actividades de EEUU y el Reino Unido, han buscado simultáneamente asegurar que las actividades de sus propios aparatos de seguridad e inteligencia nacionales se mantuvieran fuera del debate. La canciller alemana, Angela Merkel, ha hecho una gran trabajo de interpretación para las audiencias internas (la NSA 'como la Stasi", 'los amigos no se espían entre sí", etc.) mientras que ignoraba en gran medida la inquietud ampliamente compartida por la vigilancia interna y enviaba un grupo de negociadores de Washington en lo que primero pareció como un intento de garantizar la admisión de

Alemania en el club *Five Eyes*. En connivencia con el Reino Unido, el Gobierno alemán también bloqueó la rápida adopción del borrador para regular la protección de datos en la UE, solicitado por el Parlamento Europeo y la Comisión, paralizando unas necesitadas reformas largamente debatidas.

El Gobierno francés describió las prácticas de la NSA como 'totalmente inaceptables" antes de incluir en la Ley de Defensa 2014-2019 provisiones que garantiza la expansión de sus poderes a sus propios servicios de seguridad para grabar conversaciones telefónicas, acceder a emails, realizar localización y acceder a otros metadatos sin ninguna supervisión judicial. Mientras tanto el Gobierno británico, cuyo espionaje sobre sus socios comunitarios seguramente representa una transgresión contra 'amigos" de una magnitud mucho mayor a todo lo realizado anteriormente por EEUU, ha sido el más cínico al rechazar cualquier crítica, describiendo a los críticos de la GCHQ como tipos 'fantasiosos" y animando a una caza de brujas contra *The Guardian.* El socio de Glenn Greenwald[46] fue detenido en el aeropuerto de Heathrow bajo las leyes antiterroristas y bajo la supervisión de agentes estatales destruyeron un portátil propiedad del periódico. Todo ello no presagia nada bueno sobre el estado de la democracia en ese país.

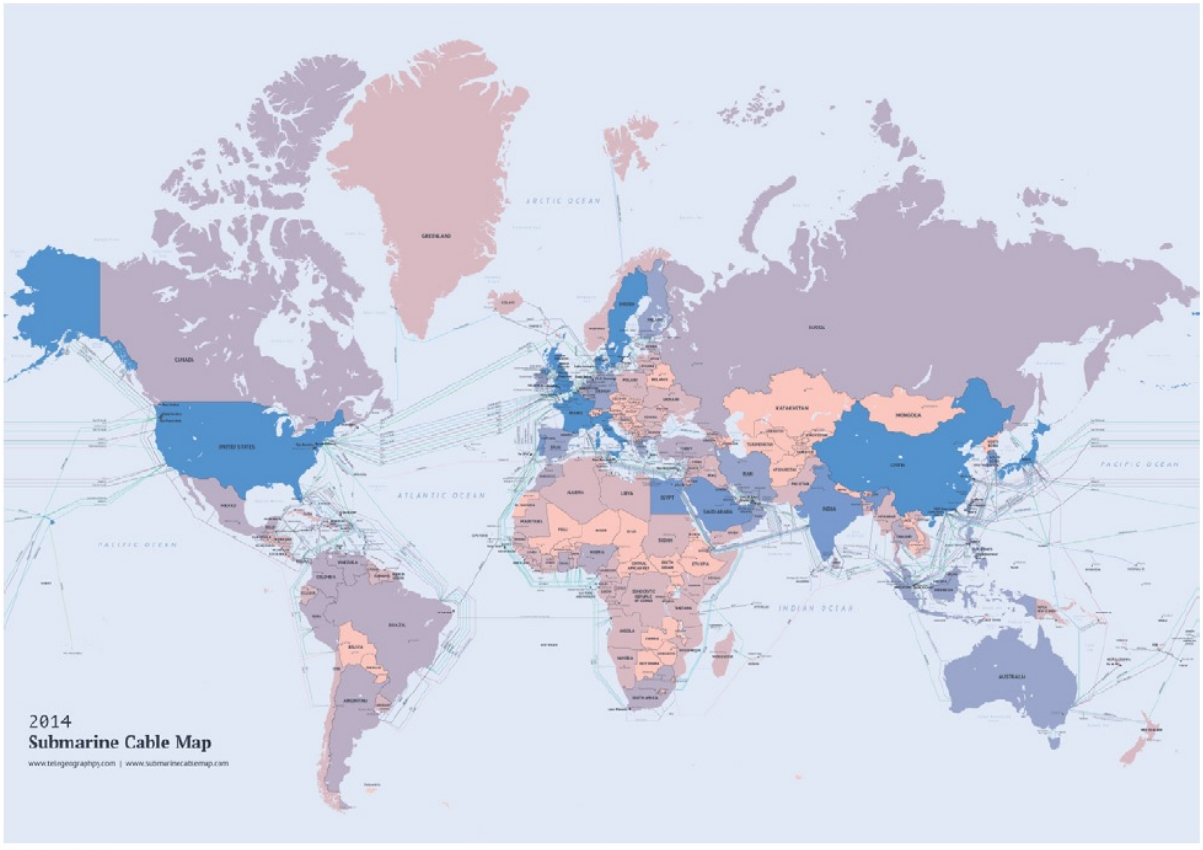
La Comisión Europea, desprovista de cualquier poder en lo que respecta a las políticas de seguridad nacional de los Estados miembro de la UE, ha sido muy franca sobre el espionaje de la NSA, pero en la práctica se ha reducido a lanzar amenazas y desaprobaciones señalando con el dedo en la dirección de Silicon Valley, lo que es un poco inconsistente, ya que algunos de los acuerdos de vigilancia de las comunicaciones en Europa son igual de problemáticos. El Tribunal de Justicia de la UE ha indicado que muy probablemente anulará una directiva impulsada por la Comisión que obligaba a los servicios de telecomunicaciones y grandes suministradores de internet a conservar por ley los metadatos durante 24 meses con fines de seguridad; esta decisión se debe a que no fue capaz de hacer un seguimiento judicial adecuado (o, de hecho, estipular cualquier restricción sobre el acceso a datos).

El Parlamento Europeo ha completado una investigación sobre la vigilancia de la ciudadanía comunitaria por la NSA y sus homólogos europeos, pero sin el poder para obligar a los testigos a declarar, ha dependido de periodistas, promotores de campañas y expertos independientes. Su borrador de recomendaciones, que no son vinculantes en la UE, incluirían probablemente la suspensión de varios acuerdos para compartir datos con EEUU hasta que se implante la privacidad recíproca y derechos de protección de datos, el desarrollo de una 'nube de la UE" y la reforma de los programas europeos de vigilancia masiva.

[46] Glenn Greenwald es un abogado constitucionalista estadounidense, columnista, bloguero y escritor. Desde agosto de 2012 hasta octubre de 2013 fue columnista de la edición estadounidense de The Guardian. Fuente: Wikipedia (N. de la T.).

En lo que respecta a EEUU, a pesar de todas las opiniones sobre el terrible estado de la democracia en el país, va muy por delante de los Estados miembros de la UE en lo referente a las reformas internas que pueden ser necesarias para proteger a sus ciudadanos de las extralimitaciones de la inteligencia. Un juez federal ha emitido una norma preliminar en la que señala que la recopilación masiva de registros telefónicos viola probablemente la Constitución de EEUU, calificando la práctica de 'indiscriminada", 'arbitraria" y 'casi orwelliana". Este sentimiento tuvo eco en un Informe presidencial del Grupo de Inteligencia y Tecnologías de Comunicaciones, cuyas 46 recomendaciones, si se implementan al completo, conducirá al menos a frenar los poderes de vigilancia de la NSA. El tiempo dirá si Obama da la batalla; los antecedentes históricos no son muy alentadores.

Mapa de comunicaciones por cable submarino



Telegeography 2014

Legalidad internacional vs. seguridad (trans)nacional

La cuestión es si vivimos en un mundo donde la NSA y sus aliados pueden hacer lo que quieran en internet y los secretos que guarda, o si se trata de respetar el Estado de derecho y los principios universales de derechos humanos, en concreto, el derecho a la privacidad, un derecho del que dependen muchos otros. Como señaló Edward Snowden,

«No quiero vivir en un mundo en el que todo lo que diga, lo que haga o todos aquellos a los que hable, cada expresión de creatividad, de amor o de amistad sea grabada».

Los límites a los poderes 'internos" de espionaje están recogidos en mayor o menos medida en las constituciones nacionales, que deben garantizar claramente a los ciudadanos derechos de privacidad y la protección contra interferencias indebidas del Estado. Mucho más problemático es que las personas originarias de otros países –que habitualmente no disfrutan de los mismos derechos de ciudadanía– pueden convertirse fácilmente en objeto de vigilancia por parte de algún Estado. Se trata de una cuestión crucial por dos razones. Primera, las comunicaciones digitales con frecuencia pasan a través del territorio o jurisdicción de diferentes países, particularmente por EEUU, destino de la mayoría del tráfico mundial de internet. Esto significa que si no eres un ciudadano estadounidense, cualquier derecho constitucional de privacidad que puedas tener en tu país de origen es prácticamente inservible a medida que navegas amplias áreas de internet. Segunda, mientras que el principal protagonista del caso de los archivos de la NSA es, por supuesto, EEUU, esa agencia figura en el centro de una red de inteligencia transnacional de alcance global que aún se guarda en secreto y que opera prácticamente sin regulación. Esta es la razón, según Privacy International, de que abrir *Five Eyes* sea un prerrequisito para restringir sus poderes de forma significativa.

El comité de evaluación de la administración Obama sorprendió a algunos recomendando que la vigilancia a ciudadanos no estadounidenses fuera sometida a controles más estrictos y que su derecho a la privacidad fuera reconocido, pero, de hecho, descartó dar protección judicial a personas objeto de vigilancia extranjera y propuso rebajar el umbral para considerar una 'creencia razonable" (más que causa probable) de vigilancia requerida en interés de la seguridad nacional. Tampoco las personas fuera de EEUU se benefician de las obligaciones propuestas por la NSA para minimizar los datos guardados de ciudadanos estadounidenses.

Es improbable que esto satisfaga a los críticos europeos de las prácticas de EEUU o a los del Gobierno brasileño, que demanda que todos los proveedores de servicios de telecomunicaciones extranjeros que operan en Brasil tengan sus servidores en ese país, de modo que los datos de sus ciudadanos estén sujetos exclusivamente a la ley brasileña. Con la amenaza de otros países de actuar en la misma dirección, no son solo las empresas las que previenen para que se evite la 'balcanización" de internet, a medida que las normas actuales y los estándares técnicos quedan pulverizados.

Mientras que 'el verano de Snowden" demostró el poder de la NSA y de las grandes compañías tecnológicas, también ha mostrado la debilidad de la normativa internacional y del actual sistema de gobernanza. La legalidad y jurisprudencia de

derechos humanos deja poco margen de duda de que lo que *Five Eyes* y otras estructuras han estado haciendo contraviene tanto la letra como el espíritu de la legalidad internacional. No se trata solo de que han sido ignorados los estándares de derechos humanos; la cuidadosa elaboración de marcos de asistencia legal mutuos (que permiten a los Estados solicitar y acceder a información o evidencia mutuamente sobre sus respectivos ciudadanos) durante décadas se han adelgazado desde el 11-S.

Los defensores de la gobernanza global deberían estar reclamando acuerdo internacionales que limiten la vigilancia al tiempo que consagren los derechos individuales de privacidad y el proceso debido, pero actualmente es inconcebible que los Estados acepten cualquier tratado internacional que pretenda limitar sus estructuras de seguridad. Es fácil de anticipar que las corporaciones que manejan estas enormes cantidades de información se resistirán a cualquier intento de regular el derecho a la privacidad o la protección de datos en la legalidad internacional. A pesar de todo el debate en torno a la reforma sobre la vigilancia, es significativo que los principios de Silicon Valley no hagan mención en absoluto a ningún derecho individual, digital o de otro tipo. Sin embargo, existe un apoyo tangible y creciente hacia tales medidas.

La Asamblea General de la ONU ha aprobado recientemente una Resolución pionera (propuesta por Alemania y Brasil) sobre 'El derecho a la privacidad en la era digital", aunque solo vinculante para el Alto Comisionado para los Derechos Humanos de la ONU, que recibirá el encargo de preparar un informe sobre el asunto. También se ha sugerido un nuevo protocolo opcional de la Convención Internacional de Derechos Civiles y Políticos, pero incluso si logra congregar a la clase política, en el mejor de los casos, llevará años alcanzar un acuerdo, y mucho más ratificarlo. En el corto plazo, las medidas nacionales que limitan la vigilancia por parte de agencias de inteligencia son la única vía significativa de reforma.

Agujas vs pajares

Las revelaciones de Edward Snowden ya han inspirado una serie creciente de retos legales y los tribunales en Europa y EEUU se encuentran ante la petición de sopesar la legalidad de lo revelado, que contravienen las leyes de respeto a los derechos humanos y al proceso debido. Se trata de la encarnación más reciente del debate, ya con una década de antigüedad, sobre la necesidad de equilibrar libertad y seguridad y las nuevas prácticas introducidas bajo la guerra contra el terror. La libertad ha estado mucho tiempo en la parte perdedora; es de esperar que Snowden haya revertido esta tendencia. En la arena política este debate ha tomado la forma de lucha contra la vigilancia masiva e indiscriminada y a favor de leyes que limiten la vigilancia solo a los casos estrictamente necesarios, una vigilancia enfocada y proporcionada.

Lo que a menudo ignoran estos debates es el cambio fundamental de lo que hoy implica la seguridad nacional, desde la recopilación de datos intensiva en empleo de la era Hoover y MacCarthy a los grandes bancos de datos y procesamiento intensivo de información de la NSA que dirige actualmente Keith Alexander. En este sentido, la lucha de poder se establece actualmente entre el sistema de controles y contrapesos de la democracia liberal del siglo XX, enraizados en los Estados-nación y la regulación de poderes investigativos, y un nuevo modelo basado en la vigilancia masiva transnacional y 'preventivo" desarrollado en el siglo XXI. La dificultad de tratar de hacer que este nuevo modelo respete las tradicionales nociones de causa probable y proceso debido surge del hecho de que muchos de los métodos que utiliza son antitéticos a tales nociones.

La prevención ha estado durante mucho tiempo en el núcleo de la misión de seguridad nacional del Estado. Mientras que la vigilancia policial en una investigación por actividades criminales debe iniciarse sobre la base de que existe una 'causa probable" que un sospechoso merece atención, seguido de autorización judicial para evitar medidas intrusivas, las agencias de seguridad nacional se ocupan básicamente de identificar amenazas y mitigar riesgos antes de que se materialicen. Después del 11-S este paradigma de gestión del riesgo se ha extendido por todo el aparato de la seguridad nacional hasta englobarlo todo, desde la detención preventiva a las listas negras secretas y los asesinatos extrajudiciales por ataques de *drones*, atizando la represión estatal en todo el mundo y promoviendo el cerco a cualquiera que desafíe al *statu quo*.

Forzados por primera vez a defender sus programas de recopilación masiva de datos, los jefes de inteligencia han repetido el mismo mantra una y otra vez: «necesitamos el pajar para encontrar la aguja». En consecuencia, se argumenta que cualquier freno a la vigilancia compromete la seguridad nacional. Mientras que esta afirmación puede resultar una defensa conveniente de la vigilancia masiva, la realidad es que la policía y los servicios de inteligencia han accedido por igual desde hace mucho a los 'pajares" en una lógica de caso por caso, o incluso de forma amplia; lo que Snowden ha revelado es la construcción de un pajar masivo compuesto por tantos datos históricos como sea posible que permitan a la NSA y sus aliados rebobinar literalmente lo que sus ciudadanos han estado haciendo en momentos concretos.

La primera prueba para una reforma significativa de la vigilancia se concreta en que las agencias de inteligencia den por terminada la recogida masiva de datos. Dada la cultura de la vigilancia entre cientos de miles de agentes estatales y contratistas y la infraestructura en la que ha invertido la NSA para facilitar esta vigilancia masiva (acaba de construir uno de los centros de almacenamiento de datos más grandes del mundo en Utah), no debemos subestimar la magnitud de esta tarea. La segunda es evitar que las agencias estatales accedan a grandes bolsas de datos –no solo metadatos de

comunicaciones, sino datos financieros, de viajes, de salud, etc.– en ausencia de una razón legítima para hacerlo y una vigilancia efectiva de esas peticiones. Si vamos a proteger la presunción de inocencia y el derecho a la privacidad en un entorno de grandes cantidades de datos, entonces en último término necesitamos cortafuegos que limiten tanto la evaluación por perfil como que eviten las 'expediciones de pesca" diseñadas para obtener motivos de sospecha entre los inocentes.

La tercera prueba apunta a circunscribir las condiciones bajo las que las agencias de seguridad e inteligencia pueden acceder a estos datos para satisfacer su cometido. Este desafío necesita tanto más transparencia por parte de aquellos que realizan la vigilancia (necesitamos saber quién y cómo se utilizan los 'pajares" en la práctica) como una distinción mucho más clara entre los asuntos de seguridad nacional, por una parte, y la recogida de datos de inteligencia criminal por otra. Se trata realmente de determinar qué grado de la 'guerra contra el terror" debe ser gestionada por agencias secretas de inteligencia y militares y qué grado debe ser procesada dentro de un marco del Estado de derecho. El cuarto reto es reemplazar los acogedores comités parlamentarios favorables al *establishment* que actualmente tienen la tarea de vigilar a estas agencias a través de sensatos mecanismos de control democrático.

En última instancia, el actual debate sobre la aguja y el pajar gira en torno a cuántos datos (si es que alguno) deberían ser retenidos por las compañías que los almacenan o transportan con propósitos legales o de seguridad y las circunstancias bajo las cuales puede accederse a ellos. El peligro reside en los pretextos y trucos que pueden normalizar la situación existente en lugar de examinar lo que se ha revelado. El panel de valoración de la NSA de Obama propuso poner fin a la recogida masiva de metadatos por la NSA, pero a cambio los proveedores de servicios los pueden conservar 30 meses y tener acceso a los datos controlados por los (tradicionalmente permisivos) tribunales de vigilancia.

Como se señaló anteriormente, la UE puede estar avanzando en la dirección opuesta: la recomendación de su Tribunal de Justicia ha visto con malos ojos su Directiva de Retención de Datos y el principio de conservar los datos mucho tiempo solo por si pueden resultar de utilidad a la policía y a agencias de seguridad.

Al final, ambas partes tendrán que resolver al menos algunas de sus diferencias en relación a los poderes de vigilancia y protección de la intimidad/privacidad si se ha de mantener o profundizar la cooperación UE/EEUU. Esto puede incluso mejorar las perspectivas para el desarrollo de un acuerdo internacional sustantivo a largo plazo.

El Estado dentro del Estado en el que estamos

En la mayoría de demandas por la reforma en la vigilancia post-Snowden aparece casi en la cima de la lista más transparencia y control de los servicios de inteligencia. Sin embargo, se constata la falta de voluntad política a la hora de examinar cómo las democracias liberales han permitido a sus aparatos de inteligencia hacerse tan extraordinariamente poderosos y sin controles. Como escribió un ex juez británico después de las filtraciones de Snowden, «los aparatos de seguridad en muchas democracias son hoy capaces de imponer su poder sobre otros órganos del Estado que precisan de autonomía: promoviendo legislación que prioriza sus propios intereses sobre los derechos de los individuos, dominando el proceso de toma de decisiones al máximo nivel, excluyendo a sus antagonistas fuera de los procesos judiciales y operando prácticamente sin escrutinio público».

Esto es lo que combaten las campañas para la reforma de la vigilancia; es ingenuo pensar que las demandas de un mayor control a los poderes de vigilancia tendrán éxito fácilmente después de una década de intentos para que EEUU y sus aliados respondan por su papel en las 'entregas extraordinarias", tortura, detenciones ilegales secretas, internamiento y crímenes de guerra bajo la guerra contra el terror se han encontrado con tal resistencia (por no mencionar la conducta criminal que se remonta a mucho antes del 11-S). A lo largo de Europa y América del Norte, interrogatorio tras interrogatorio, juicio tras juicio, la ley ha dictaminado en la mayoría de los casos que se rectificara, mientras los Estados han cerrado filas y los gobiernos han adoptado una posición defensiva, ignorando o exonerando las acciones de sus agencias de inteligencia y seguridad. ¿Por qué? Porque los aparatos de seguridad nacional y de inteligencia internacional están íntimamente implicados en todo lo que los Estados hagan militarmente y en muchas de sus intereses y políticas económicas e internacionales. En geopolítica, las estructuras de vigilancia, o 'conocimiento situacional", está en el corazón de la proyección del poder duro y blando.

Otro tema fundamental en relación a muchos de los actuales llamamientos a la reforma en la vigilancia es que tratar de introducir de algún modo los mecanismos de control y contrapesos dentro de las agencias de vigilancia, que operan en secreto para adelantarse a las 'amenazas" de enemigos conocidos y desconocidos, inevitablemente se convierte en un ejercicio contradictorio: llevado a su conclusión lógica, el argumento de que toda vigilancia debe ser necesaria, proporcionada y bajo un adecuado control democrático y judicial es realmente una razón para restringir de forma radical el mandato y poderes de los servicios de inteligencia y asignar en su lugar a la policía y a los servicios de investigación criminal problemas como el del terrorismo. Gracias a la obsesión cercana al culto con la (in)seguridad en los medios de comunicación tal pretensión se equipara con la blasfemia.

Quizá esta es la razón por la que tantos activistas hablan de la vigilancia como si ocurriera en un vacío, ignorando el asombroso desarrollo de los aparatos de seguridad nacional, en particular desde el 11-S, su impacto sobre 'comunidades sospechosas" y su relación con estrategias para luchar contra la 'radicalización" y el 'extremismo interno". El moreno es el nuevo negro, y el verde es el nuevo rojo.[47] En todo el mundo, la protesta pacífica y desobediencia civil que los demócratas afirman respetar es atacada como nunca por aquellos que (lógicamente) los partidarios de una acción directa más pacífica califican como 'extremistas", o incluso 'terroristas". La lucha contra la vigilancia sin control debe estar en el núcleo de las luchas por la justicia social.

También podemos preguntar cómo es que el neoliberalismo ha logrado capturar tantos servicios públicos bajo la retórica del despilfarro y ineficiencia, mientras que los 'Altos sacerdotes de los Estados securitarios" pueden gastar a su antojo incontables billones en ejércitos de contratistas e instalaciones ideadas por diseñadores de los decorados de Hollywood. Después de asistir a MILIPOL, la XVIII edición de la exposición mundial de 'seguridad interna para los Estados" en París, encuentro más difícil que nunca evitar la simple conclusión de que la razón es que lo que es bueno para la seguridad del Estado es bueno para los negocios, y viceversa.

La seguridad nacional, centrada en su mayor parte de una u otra forma en técnicas de vigilancia masiva, ya es un negocio multimillonario. Con él llega la difuminación creciente de los límites entre el ejército, la seguridad nacional y el orden público, y la manía por todo tipo de cachivaches, desde *drones* a armas 'menos letales", tecnologías de control de masas, aplicaciones de vigilancia masiva, controles fronterizos militarizados y todo lo demás en el escaparate de MILIPOL.[48] Me pregunto cuántos de los grandes actores estarán ahora en Davos esgrimiendo el miedo y la inseguridad para vender lo que en la feria se parece bastante a los poderosos tratando de protegerse a sí mismos de los débiles.

El emperador lleva ropa de diseño y armadura de diseño. Debe suponerse que una ya poderosa industria de la vigilancia querrá llenar cualquier hueco de 'seguridad" dejado por el control democrático en el Estado de la vigilancia. Si somos serios en nuestro propósito de limitar la vigilancia, necesitamos restricciones serias tanto del Estado como del sector privado.

---

[47] La frase alude al hecho de que las personas de tez morena, en especial asiáticas y latinas, son las principales víctimas del racismo en Estados Unidos actualmente; por su parte el ecologismo y sus activistas han pasado a heredar el estigma que tuvo el comunismo en su día. Ver, por ejemplo: http://bgpappa.hubpages.com/hub/Racism-In-America-Brown-is-the-new-Black y http://www.motherjones.com/mojo/2011/05/green-new-red-crackdown-environmental-activists .

[48] Véase además B. Hayes, *NeoConOpticon,* TNI y Statewatch, 2009. Disponible en: http://www.tni.org/report/neoconopticon

Poder y autonomía bajo el capitalismo digital: ¿la mercantilización de los derechos?

La vigilancia masiva y globalizada ha emergido porque los acuerdos internacionales diseñados para prevenir la aparición en Europa de Estados autoritarios en los albores de la segunda guerra mundial no han logrado, precisamente, controlar la consolidación de esta clase de poder ilegítimo, en particular desde el final de la guerra fría. Entidades como la UE y la ONU, capturadas por corporaciones o pequeños grupos de países poderosos, han acelerado estos procesos sin proponérselo. Los que controlan los grandes bancos de datos han garantizado todos los derechos y toda la información. La privacidad se ha convertido en algo a lo que optas: evitando algunos servicios y haciendo uso de otros. También hay un mercado para esta clase de 'seguridad"; simplemente todavía no goza del apoyo gubernamental y las subvenciones públicas que disfruta la industria de la seguridad.

En un artículo en *The Financial Times*, el astuto inconformista Evgeny Morenov criticaba la estrecha visión de los debates sobre el 'alcance de la inteligencia" argumentando que todos, incluido el mismo Snowden, se han equivocado en el punto clave sobre el mundo de la vigilancia masiva que él denunció: «la tendencia mucho más preocupante por la cual la información personal sobre nosotros, más que nuestro dinero, se convierte en la principal forma de pagar por nuestros servicios, y ¿quizá pronto por los objetos cotidianos que utilizamos?».

Durante mucho tiempo se ha entendido que si un servicio es gratuito, *tú eres el producto*, pero a medida que los consumidores proporcionan más y más datos personales en retribución por capital social y ganancia material, mayor es el potencial para aquellos que controlan las grandes bases de datos para influir en el destino de estos de maneras que aún desconocemos, una premisa que, en sí misma, es profundamente antidemocrática. Para Morenov, esto constituye una «nueva tensión en los cimientos mismos del capitalismo actual y de la vida democrática». Tiene razón en que hace falta «un poco más de imaginación» para resolverlo.

Nuevas formas de guerra y de control de la población

Tica Font
Directora del Institut Català Internacional per la Pau (ICIP)

Las siguientes reflexiones giran en torno a los cambios más perceptibles que se están produciendo en el ámbito de la seguridad y la defensa, y los retos de carácter jurídico y ético que conllevan.[49] Estos cambios hay que contextualizarlos en el marco del proceso de globalización, en el marco neoliberal imperante y en el marco de post Guerra Fría. Tampoco hay que olvidar el contexto de crisis económica, las consiguientes políticas de ajustes presupuestarios y los recortes en los presupuestos de defensa.

La industria de defensa, en conjunción y simbiosis con los Ministerios de Defensa, buscan soluciones a los cambios acontecidos en los últimos 25 años. Las propuestas elaboradas apuntan, por una parte, a privatizar servicios militares, es decir, que algunas tareas propias de los militares sean llevadas a cabo por empresas, en general compañías participadas por firmas productoras de armas, y militares en la reserva que pasan a dirigirlas. La siguiente estrategia se centrará en iniciar una nueva revolución tecnológica aplicada a las armas: diseñar una nueva generación de armas robóticas que disminuyan el número de efectivos militares necesarios y los riesgos para la vida de los militares de manera que complementen sus tareas y suplan la disminución de efectivos militares.

En este nuevo contexto mundial de post Guerra Fría se han redefinido los riesgos, amenazas y enemigos que hay que combatir y las estrategias a seguir. La seguridad interior-exterior ha pasado a ser un elemento esencial en el nuevo contexto. Hoy en día la seguridad constituye una prioridad política y un gran estímulo al desarrollo de tecnologías que permitan vigilar a cualquier ciudadano, sea o no del país que está vigilando o espiando, y para generar nuevas armas, los llamados robots autónomos letales, que podrán seleccionar y atacar objetivos sin la intervención humana; esto equivale a la guerra llevada a cabo por las máquinas.

[49] Este artículo está basado en otro trabajo previo ya publicado, T. Font, «El derecho a la paz y la tendencia armamentística actual», en Fundación Seminario de Investigación para la paz (eds.), *Los Derechos humanos en tiempos de crisis*, Mira editores, Zaragoza, 2014, pp 371- 391.

Homeland Security o Estado de vigilancia

En la segunda mitad de la década de los noventa el *lobby* militar industrial, junto con los centros de creación de opinión –los *think-thank*–, empezaron a generar nuevos escenarios de conflictos, con sus consiguientes riesgos y amenazas. Junto con estas corrientes de búsqueda de polos de conflictividad mundial en el año 2001 se producirían los atentados del 11-S y el lanzamiento por parte del Gobierno estadounidense de la llamada *guerra global contra el terrorismo*.

Los acontecimientos que siguieron al 11-S impulsaron este nuevo enfoque de la seguridad. Estados Unidos reformuló el ámbito de la seguridad bajo el síndrome del terrorismo acuñando el concepto de *homeland security* (2002), una estrategia donde se combinaban aspectos policiales, militares y de seguridad en todos los ámbitos de la vida nacional, tanto del espacio público como del ámbito privado. Se crearon diversas agencias dedicadas a ejercer una estrecha vigilancia en aeropuertos, transportes, comunicaciones, transacciones financieras e internet, entre otros, mediante agencias estatales de seguridad, activos militares, empresas privadas de seguridad e industrias fabricantes de armas.

En paralelo a EEUU, los países de la Unión Europa (UE) y la OTAN abrieron la reflexión a la creación de un nuevo concepto estratégico y los gobiernos empezaron a definir sus estrategias de defensa y seguridad en el nuevo contexto internacional.

Por su parte, la UE presentó en el 2003 la Estrategia Europea de Seguridad (EES).[50] Cinco años más tarde la UE revisó la EES[51] y reafirmó las amenazas a la seguridad europea según se describe a continuación. La *proliferación de armas* de destrucción masiva, tanto en manos de terroristas como en manos de ciertos Estados, se definen como un peligro para la seguridad mundial, por ello los esfuerzos se centran en evitar que nuevos Estados tengan la capacidad de fabricar armas atómicas. El *terrorismo*, del que se señala que la UE ha actuado con decisión para proteger a la sociedad; ven necesario redoblar los esfuerzos contra la radicalización de ciertas ideologías extremistas ligadas al islamismo que fomentan la violencia. La *delincuencia organizada*: se afirma que se han de profundizar las asociaciones de seguridad interior entre los países europeos mediante una política de mayor coordinación e integración de los cuerpos policiales y judiciales, poniendo especial celo en los movimientos de personas. La *ciberseguridad*, que se considera un punto débil de las economías

[50] El Consejo Europeo adoptó la Estrategia Europea de Seguridad (EES), *Una Europa segura en un mundo mejor*, Bruselas 12 de diciembre de 2003. En ella se establecen por primera vez principios y objetivos para promover los intereses de la UE en materia de seguridad, basados en los valores esenciales de la comunidad occidental.

[51] El Consejo de Europa elabora un informe que no sustituye a la EES del 2003, sino que pretende reforzarlo. *Informe sobre la aplicación de la estrategia Europea de Seguridad- Ofrecer seguridad en un mundo en evolución*, Bruselas 11 de diciembre 2008, S407/08.

modernas, ya que dependen en gran medida de infraestructuras vitales, como transportes, comunicaciones y suministro de energía; se estima que es un ámbito que se debe reforzar para evitar ciberataques. La *seguridad energética:* existe una gran preocupación por la dependencia energética, sobre todo de la energía fósil, y por la inestabilidad de los países proveedores. En este sentido, se hace una apuesta por la diversificación de los combustibles, de las fuentes de suministro y de las rutas de tránsito; también por el buen gobierno y el respeto al Estado de derecho en los países de origen. El *cambio climático*: se percibe como un multiplicador de amenazas por catástrofes naturales, degradación del medio ambiente y competencia por recursos naturales, factores que pueden exacerbar la situación de pobreza dando lugar a crisis humanitarias, políticas y de seguridad y, aún peor, en conflictos que afectarían a las rutas comerciales de materias primas y generarían flujos migratorios en dirección a Europa.

Para llevar a cabo esta estrategia, la UE se ha dotado de un entramado de agencias y numerosos instrumentos destinados a incrementar la seguridad europea, como bien revelan todos los informes y los documentos elaborados por la Comisión; todo ello persigue la defensa del 'propio territorio" europeo y la lucha frente a las 'amenazas contra el estilo de vida occidental". Se trata de ideas ultraconservadoras que nos abocan a una peligrosa 'sociedad de la vigilancia", dotada de unos sistemas de vigilancia supraestatales que lo ven todo y lo controlan todo, como la cámara del Gran Hermano.

Hoy en día hasta los detalles más insignificantes de nuestras vidas están siendo registrados, almacenados y estudiados con fines comerciales o de seguridad, evidentemente con nuestra cooperación consciente o inconsciente. Los escáneres humanos de aeropuertos, la toma de medidas biométricas, pasaportes de identificación por radiofrecuencias, las cámaras de video de aeropuertos, centros comerciales, calles y peajes de autopistas, la geolocalización de los teléfonos móviles, las conexiones a páginas web, nuestros comentarios en Facebook o Twitter, la lectura de periódicos on-line, etc. almacenan datos de posición, tiempo, preferencias, preocupaciones, hábitos y actividad que realizamos diariamente. Todo ello permite abordar estrategias de *marketing* personalizadas, perfiles de comportamientos ciudadanos y categorizaciones.

En junio del 2013 Edward Snowden filtró documentos secretos procedentes de la National Security Agency (NSA) estadounidense. Gracias a ello supimos que EEUU, pero también países europeos, China y Rusia, interceptan sin pudor millones de llamadas telefónicas de ciudadanos de todo el mundo. Gracias a él también sabemos que durante algunos años empresas de comunicación y proveedores de internet han colaborado con los gobiernos para ceder, robar y analizar millones de datos sin ningún control político o judicial. Un año después del escándalo el debate se ha reducido a la privacidad de la línea y a la comercialización de la información.

Todo este entramado se está construyendo sin ningún control ni regulación democrática. Estos sistemas vulneran el principio de privacidad, el derecho a la intimidad y el derecho al honor, principios fundamentales de la democracia. Existe un grave peligro añadido: esta vigilancia, en muchos casos, se está llevando a cabo desde empresas privadas.

Empresas Militares y de Seguridad Privadas (EMSP)

Desde finales de los años noventa se plantea la cuestión de cómo mantener la superioridad militar en un escenario de nuevas operaciones militares y con presupuestos más bajos. La solución se busca en dos frentes. Por una parte, se centra en el aumento de instrumentos y armas de alta tecnología, con el uso de tecnologías más sofisticadas y mayor capacidad de procesamiento de datos o de armas de mayor precisión. Por otra, los esfuerzos se centran en la organización militar: cómo disminuir el número de efectivos, aligerar la estructura, privatizar algunas funciones militares e incorporar funciones policiales.

En este contexto, los gobiernos se replantearon estrategias de organización y logística militar junto con la definición de proyectos de armas que se adaptasen a los nuevos conflictos emergentes. Esta situación ha provocado, y está provocando, una presión hacia los gobiernos por parte del complejo militar industrial para que externalicen actividades militares hacia el sector militar privado.

Los gobiernos más influenciados por la corriente neoliberal privatizadora, con EEUU y el Reino Unido a la cabeza, han iniciado esta apuesta privatizadora y propician la aparición de un nuevo sector económico al que le han traspasado algunas tareas y funciones propias de los ejércitos. Ya a lo largo de la década de los noventa aparecieron empresas, muchas de ellas ligadas a la industria productora de armamento, que ofrecerían servicios de mantenimiento, suministro, modernización de equipos y armas, apoyo logístico, formación y entrenamiento militar y policial, así como construcción de bases militares y su mantenimiento en cualquier parte del mundo. Estas empresas ofrecen también servicios de inteligencia, contrainteligencia y operaciones especiales; asesoramiento estratégico y técnico a gobiernos y militares; servicios de traducción; protección de personas, instalaciones o infraestructuras; ayuda humanitaria; respuesta rápida ante desastres; apoyo en operaciones de paz; destrucción de armas; gestión de conflictos, negociaciones de paz, transiciones políticas, etc.

Estas empresas cuentan con personal especializado, generalmente ex militares, y están dotadas armamento pesado. En definitiva, se trata de empresas con capacidad suficiente para actuar en el 'campo de batalla" o en situaciones posbélicas; podemos decir que son ejércitos privados preparados para actuar en donde se les requiera.

Una de las consecuencias de privatizar el uso legítimo de la fuerza o de la violencia ha sido la aparición de numerosas denuncias de violaciones de los derechos humanos perpetradas por dichas empresas contra la población civil en aquellos lugares en los que han sido contratados para llevar a cabo trabajos desconocidos, secretos y no públicos. Veamos algunos casos.

Bosnia, 1999. Un trabajador de DynCorp denuncia y declara ante la Corte de Texas que compañeros y superiores suyos compraron y traficaron con niñas para ser utilizadas como esclavas sexuales. Las mujeres eran compradas, junto con la compra de su pasaporte, para su disfrute personal y cuando se cansaban las revendían por 600 u 800 dólares, o la alquilaban por horas o por noches a un club nocturno. Explicó que estas niñas no eran de Bosnia, sino que procedían de Rusia, Rumania u otros lugares; las adquirían a la mafia Serbia. También declaró que sus compañeros traficaban con armas ilegales y pasaportes. Ante estas revelaciones, DynCorp además de despedir al trabajador por desvelar los hechos, abrió una investigación interna que condujo al despido de dos trabajadores y su devolución a EEUU.[52] Ni la empresa ni los trabajadores han sido procesados ni encausados por estos hechos. Expertos en derechos humanos están reclamando que las empresas se hagan responsables legales de los actos de sus empleados y que los gobiernos que han contratado a dichas empresas manden un mensaje claro: la violación y vulneración de los derechos humanos es un delito en cualquier jurisdicción y que despedir a un trabajador por esclavitud sexual no es suficiente castigo.

Abu Ghraib, Irak 2003. Un militar norteamericano difunde imágenes de malos tratos, torturas y vejaciones en dicha prisión. Tres de los prisiones interponen demanda contra las empresas Titan y CACI, que en principio estaban contratadas para facilitar traductores, aunque todo parece indicar que 31 empleados de las mismas tomaron parte en las torturas. El abogado de CACI afirmó que estas denuncias eran falsas y que la empresa sirvió a su país de forma honorable mientras trabajó en Irak. El resultado del proceso judicial fue que tres militares fueron acusados, juzgados y sentenciados por cometer abusos durante los interrogatorios. Ahora bien, ningún trabajador de estas empresas ha sido juzgado por los mismos hechos.[53]

Croacia 1994. El Gobierno croata pidió al gobierno norteamericano ayuda para formar sus incipientes fuerzas armadas, pero como Croacia estaba embargada por

[52] P. Serrano, «Estados Unidos encarga a empresas de mercenarios las operaciones sucias en América Latina», Centro de Investigación sobre globalización, 5 de julio 2010. http://www.globalresearch.ca/articles/SER207A.html [Consulta 8-4-2012].

[53] Véase «Abu Ghraib inmates sue US firms», BBC, 1 de julio 2008. http://news.bbc.co.uk/2/hi/americas/7482617.stm [Consulta 1-7-2011]; y «Private Contractors and Torture at Abu Ghraib, Iraq», CorpWatch, 7 de mayo 2004. http://www.corpwatch.org/article.php?id=10828 [Consulta 11-12-2012]

Naciones Unidas, el trabajo de formación de nuevos militares se trasladó a la empresa MPRI. Durante algunos meses el ejército croata recibió formación y entrenamiento por parte del personal de la empresa. Un tiempo después, el 4 de agosto de 1995, el ejército croata llevó a cabo una ofensiva militar, llamada 'operación tormenta", con el objetivo de recuperar la Krajina, una extensa zona ocupada por serbocroatas. La operación duró cinco días. En ella se cometieron ejecuciones sumarias, asesinatos indiscriminados, desapariciones forzadas, incendios y saqueos de aldeas, y la deportación de 250.000 serbocroatas. Los mandos militares croatas que dirigieron la operación han sido procesados por el Tribunal Penal Internacional para la ex Yugoslavia y condenados por crímenes contra la humanidad. Portavoces de la empresa MPRI han negado reiteradamente su participación directa en los hechos y han sostenido que su trabajo consistió únicamente en preparar técnicamente al ejército croata. Todo ello merece una reflexión sobre la diferencia de responsabilidad que hay entre formar y entrenar para disparar y apretar el gatillo.

Privatizar servicios públicos siempre conlleva polémica y controversia, pero en este caso estamos hablando de la contratación de empresas privadas para actuar directamente en el campo de batalla, ejerciendo o pudiendo ejercer el uso de la fuerza, incluso con violencia, lo que les concede un papel muy directo en el devenir de los combates y del conflicto armado. La contratación y el despliegue de EMSP tiene un profundo impacto en cómo se ejerce el monopolio del uso de la fuerza y su control. Tengamos presente que estas empresas no rinden cuentas al Parlamento o a la ciudadanía, solo ante su accionariado. Por tanto, se agranda la distancia entre la toma de decisiones, su implementación y la rendición de cuentas.

Además, diversos estudios han recogido singularidades contractuales. Los contratos que se han llevado a cabo con el Departamento de Estado o el Departamento de Defensa de EEUU son secretos, pero por comentarios aparecidos en la prensa de directivos de las EMSP y del propio Congreso estadounidense, se sabe que dichos contratos de servicios contienen artículos que conceden inmunidad e impunidad a la empresa y a sus trabajadores frente a enjuiciamientos en tribunales locales o estadounidenses, ya sean civiles o militares.

Privatizar el uso legítimo de la fuerza contribuye directamente al debilitamiento del Estado. Uno de los pilares fundamentales de la construcción del Estado moderno y un elemento definitorio del Estado de derecho. Justamente, fue el sometimiento del poder de coerción, militar y policial, que tiene el poder ejecutivo a los poderes legislativo y judicial uno de los principales rasgos del Estado moderno. Desde esta perspectiva, privatizar o delegar el poder de coerción a entes privados supone un atentado y el desmoronamiento de los fundamentos del Estado moderno, del Estado de derecho y del respeto a los derechos humanos.

Generación de nuevas armas altamente tecnológicas. Robótica

La Administración de Barack Obama suavizó el impulso unilateralista inicial de la etapa de George Bush Jr. eliminando las 'guerras preventivas" que llevaron a EEUU a invadir Afganistán e Irak. Sin embargo, sigue manteniendo una 'guerra quirúrgica" o una 'microguerra".[54] Se trata de una guerra no convencional que no se circunscribe a un territorio o Estado concreto, sino que se libra dentro de una lucha política y militar multifacética contra el terrorismo de Al Qaeda y sus partidarios en cualquier lugar del mundo. Es una guerra secreta, invisible, de baja intensidad llevada a cabo con una nueva generación de armas muy sofisticadas, como son los *drones*. Se trata de aviones no tripulados, teledirigidos, armados con misiles y que están siendo utilizados para perpetrar ataques periódicos en, al menos, Afganistán, Pakistán, Yemen y Somalia.

Los aviones no tripulados (*drones*) o sistemas no tripulados (UAV en inglés) son aparatos equipados con sofisticados sensores, pueden ser invisibles a los radares, son capaces de ver de día y de noche, con lluvia, sol o nubes, y no se cansan ni se aburren trabajando. Estos aviones van equipados con cámaras de alta tecnología y pueden visualizar mapas de extensas regiones en 3D en tiempo real, procesar grandes cantidades de información visual, electrónica o interceptar conversaciones de teléfono móvil con o sin la ayuda de los proveedores de red. Toda esta información la transmiten vía satélite para ser procesada en grandes ordenadores (*Big Data*). La rapidez en procesar toda la información disponible es un aspecto esencial, ya que de ello depende la decisión de apretar o no el botón de disparar del operador de turno.

El modelo Predator está dirigido desde tierra y el soldado que lo opera está sentado a miles de kilómetros detrás de una pantalla similar a las de las PlayStation. Estos modelos no son rápidos ni ágiles, pero su poder está en la habilidad de ver y procesar información. Modelos posteriores, como el Reaper[55] (fabricado por General Atomics), es más inteligente, más autónomo y tienen más alcance que sus antecesores: pueden despegar, aterrizar y sobrevolar por sí mismo hacia un destino especificado –es decir, ya disponen de un buen grado de autonomía–, además de ir equipados con misiles. El soldado programa un destino o un área a patrullar y el avión ejecuta la programación mientras el militar puede concentrarse en otros aspectos de la misión. El Reaper está capacitado tanto para la vigilancia como para el ataque; está concebido para operaciones de gran altitud y larga duración: puede volar durante 27 horas seguidas a una velocidad de 450 km/h y una altitud de 15 km transportando hasta seis

[54] La nueva estrategia se formuló en el documento *Quadriennal Defence Review* (QDR) de marzo de 2010. En ella se establece la guía de los planes militares de EEUU para los siguientes cuatro años, y definía a EEUU como un país en guerra en Irak y en Afganistán.

[55] Véase https://www.google.es/search?q=MQ-9+Reaper&tbm=isch&tbo=u&source=univ&sa=X&ei=C9x7Ut2JKKrO0wX7rYGwBg&ved=0CC0QsAQ&biw=1280&bih=633

misiles. La empresa Northrop Grumman ha diseñado un *drone* silencioso de combate, el X-47B,[56] para la marina de EEUU. Ese avión ya ha realizado su primer vuelo con éxito desde un portaaviones y ha sido capaz de despegar, llevar a cabo su misión, aterrizar y reabastecerse en vuelo de manera autónoma. Lockheed Martin ha anunciado que está trabajando en un prototipo de UAV el SR-72 hipersónico que podrá alcanzar velocidades de 6 Mach –seis veces la velocidad del sonido–, de manera que ningún adversario reaccionará lo suficientemente rápido como para interceptarlo y podrá penetrar en cualquier espacio aéreo portando misiles hipersónicos.[57] En términos militares, el peor escenario es que un *drone* sea derribado, que caiga en manos del enemigo o que sea interferido.

Este tipo de aviones han sido utilizados, principalmente por EEUU, para identificar y localizar a presuntos terroristas o combatientes armados señalados. Una vez localizados, se envían los *drones*, se identifica al sospechoso y se disparan los misiles. Este uso del *drone* tiene mayor parecido a una operación policial que acaba en asesinato que a un acto de guerra.

El estupor que estas acciones causan han conducido a centrar el debate en la legalidad o no de los propios *drones*, pero la tecnología no debe ser utilizada para desviar la atención del problema: la cuestión de fondo no está en el arma, sino en el uso que se haga de ella. Estas actuaciones vulneran los principios de legalidad más elementales. En primer lugar, producen ejecuciones sumarias, extrajudiciales: se asesina a personas sin mediación de tribunales, sin juicio y sin derecho a la defensa; simplemente, alguien del Gobierno estadounidense o de la CIA decide quién ha de morir. En segundo lugar, vulneran normas del derecho internacional, como la soberanía: se sobrevuelan territorios de Estados soberanos sin el consentimiento de sus gobernantes, o se lleva a cabo un *ataque quirúrgico* contra ciudadanos de un tercer país con o sin el consentimiento del Gobierno correspondiente.

Junto a las consideraciones morales, el segundo elemento de debate sobre el uso de los *drones* con fines militares es de índole política. Los *drones* son un paso más en la estrategia de *cero bajas propias* al sustituir por máquinas ciertas funciones que realizaba el personal militar. Así, se evita arriesgar la vida de los soldados en operaciones de combate, lo que amplía el margen de maniobra de los gobiernos a la hora de decidir si se involucran en acciones de combate. Al eliminar la posibilidad de las bajas o la amenaza de que militares propios caigan prisioneros los gobernantes evitan el escándalo político y las críticas de la oposición y de la población.

[56] Véase http://actualidad.rt.com/actualidad/view/94458-x47b-drone-eeuu-portaaviones-video
[57] Véase http://www.infodefensa.com/?noticia=lockheed-desarrolla-un-uav-que-doblara-la-velocidad-de-vuelo-record-del-sr-71

Por todo ello, este tipo de armas será relevante en escenarios de intervenciones internacionales de países occidentales con misiones de apoyo a gobiernos o milicias locales, contribuyendo al éxito de la misión con un coste político ínfimo. Conviene recordar que, dado que no hay bajas, se produce un apagón informativo en nuestros países, por lo que se eliminan posibles encuestas de opinión negativas a la intervención militar y hacen que la guerra sea aceptable socialmente.

Los *drones* son el primer eslabón de una nueva generación de armas: los robots autónomos letales. Aunque todavía no muy desarrollados, los nuevos prototipos disponen cada vez de mayor grado de autonomía y llevan a cabo muchas de sus tareas de manera independiente, si bien aún precisan de intervención humana para supervisión y para tomar la decisión de disparar. Sin embargo, la nueva generación de armas, los llamados robots autónomos letales, una vez activados podrán seleccionar y atacar el objetivo precisado sin la intervención humana y estarán programados para tomar sus propias decisiones.

Esta nueva generación de armas abre un debate jurídico alrededor de tres principios. El principio de *responsabilidad*: un robot es evidente que no tiene capacidad legal, por tanto no puede ser responsable de sus acciones. Si comete un error o un acto clasificable como crimen de guerra, ¿quién será el responsable? ¿El programador informático? ¿El fabricante? ¿El militar? ¿El político que autoriza su uso? ¿Y si es usado por un actor privado? Identificar en quién recae la responsabilidad de los actos cometidos por un robot autónomo es fundamental para garantizar la rendición de cuentas y asumir las consecuencias penales que pudieran derivarse.

En segundo lugar, el principio de *proporcionalidad* exige que antes de atacar se debe evaluar el daño que pueda causar a la población civil con respecto a la ventaja militar obtenida con la acción. La proporcionalidad es propia del discernimiento humano y se basa en conceptos como el sentido común, actuar de buena fe o que la orden sea razonable. Para determinar si una ataque ha sido proporcional es necesario examinar si la persona que ha tomado la decisión de atacar estaba razonablemente bien informada de la situación, de las circunstancias o si ha hecho un uso razonable de la información disponible. La cuestión estriba en determinar si los robots pueden ser programados para replicar procesos psicológicos en los juicios de valor humanos necesarios para evaluar la proporcionalidad de una decisión.

En tercer lugar, el principio de *distinción* entre combatientes y otros actores como insurgentes, civiles, niños, mujeres ancianos, etc. El robot no solamente tiene que ser capaz de distinguir si el objetivo es un combatiente o no, sino que también tiene que hacer un balance de intenciones. En los conflictos actuales no es fácil identificar a los combatientes, ya que a menudo no llevan uniforme o insignias distintivas y suelen mezclarse con la población civil.

Estos tres principios son el fundamento del Derecho Internacional, del Derecho Internacional Humanitario y de la Convención de Ginebra. La cuestión a debate estriba en si es posible que los algoritmos de programación de los robots cumplan estos tres principios. Algunos confían en la ciencia y aseguran que será posible; los que no confían tanto apuestan por la prudencia y piden que se paren las investigaciones en armas robóticas letales, mientras que los más radicales piden que se prohíba la investigación y producción de dichas armas.

En el terreno moral, las armas autónomas representan una deshumanización de la guerra. Es cierto que los humanos bajo ciertas condiciones –calor, rabia, miedo, ira, rencor o deseo de venganza- actuamos de la peor manera, mientras que los robots, al no tener sentimientos, evitarían muertes innecesarias. También es cierto que los humanos en situación de conflicto cometen vilezas, violan a mujeres o torturan, en tanto los robots, si no están programados para ello, no causarían daños intencionadamente a la población. Algunos dan un paso más y afirman que los robots pueden cumplir con el Derecho Internacional Humanitario mejor que los humanos al no estar condicionados para preservarse a sí mismos. Este razonamiento elevado a la enésima potencia conduce a que los robots actuando en contexto de guerra pueden reducir las muertes ilegítimas o accidentales, producir menor destrucción y, por tanto, actuar mejor que los humanos. En definitiva, sus defensores presentan a los robots como una fuerza *civilizadora*.

Sin embargo, conviene considerar que las emociones son una salvaguardia; sin ellas, se puede matar más fácilmente. Los robots no pueden tener sentido común, no pueden sentir compasión, lástima, empatía, no pueden tener intuición, al igual que no puede usar trucos psicológicos, como ganarse la confianza del adversario.

Decidir sobre la vida o la muerte de las personas puede requerir visión de conjunto, de comprensión de intenciones, de previsión de acontecimientos, de intuición; los robots no pueden prever las consecuencias de sus actos; los humanos sí. Los robots pueden abordar y evaluar situaciones de forma cuantitativa, pero difícilmente de forma cualitativa, y esta es una habilidad necesaria cuando se trata de valorar sobre la vida o la muerte de las personas. Lo mismo podemos decir sobre la capacidad de distinguir y evaluar órdenes lícitas o ilícitas, o estimar e interpretar un contexto en cálculo de valores.

El desarrollo de esta nueva generación de armas ayuda a eliminar el obstáculo político para hacer la guerra. Además, eliminan la distancia física y emocional del campo de batalla y representan la cultura del *low-cost*: para Obama usar *drones* evita la muerte de soldados, disminuye el coste político de hacer la guerra y disminuye la carga moral y ética de la guerra.

Conclusiones

Riesgos como la ciberguerra, la ciberdelincuencia o el terrorismo son utilizados por los gobernantes y la industria de seguridad para justificar las ingentes partidas presupuestarias dirigidas a desarrollar tecnologías de vigilancia y tratamiento de grandes cantidades de información *(Big Data)* que supuestamente nos han de proteger de 'los otros". Pero las imágenes y datos grabados con los nuevos sistemas de vigilancia no muestran las intenciones, los motivos o las elecciones personales que hay en ellas, lo cual puede llegar a conducir a que se categoricen a muchas personas como sospechosos. Lo que no podemos saber es cuándo las categorías de riesgo pueden incluirnos 'accidentalmente", excluirnos de la entrada a un lugar o privarnos de un derecho.

La creencia de que las tecnologías de la vigilancia más grandes, más rápidas, y mejor conectadas al servicio de la seguridad pueden garantizar la paz, constituye un claro error que impide elegir otras opciones. Si queremos que la vigilancia que se está implantando no cree más inseguridad, no genere más miedo y no aumente la exclusión es necesario que libremente, voluntariamente, no cooperemos y no cedamos información a las grandes redes de vigilancia y que exijamos a los gobiernos mayor control en la protección de la información que los operadores disponen sobre todos nosotros.

Privatizar el uso de la fuerza afecta a uno de los pilares fundamentales del Estado moderno, el sometimiento del poder ejecutivo y del de coerción al poder legislativo y judicial. El ejecutivo es el que impulsa el marco jurídico que define y regula cualquier actividad empresarial, de manera que según la legislación vigente, las EMSP son empresas legalmente constituidas; pero es el propio poder ejecutivo el que ha renunciado a regular el marco de actuación concreto en el que operan específicamente las EMSP, siendo el ejecutivo al mismo tiempo el principal cliente de las mismas.

El hecho de que el Estado delegue a un ente privado un elemento definitorio de su poder y uno de los fundamentos del Estado moderno, representa una transformación en el modelo de Estado de enorme calado que requiere un amplio debate. En este escenario, conviene hablar públicamente sobre aquellas tareas que son esenciales para la seguridad y que el Estado no puede delegar, externalizar, ni privatizar.

Dada la íntima relación que existe entre las EMSP, la industria de armas y el estamento político y militar, la participación de estas empresas en un conflicto armado, ya sea utilizando la violencia o bien dando apoyo a la capacidad de llevarla a cabo, pueden acabar favoreciendo que los intereses económicos de las EMSP impulsen o

perpetúen los conflictos, o acaben generando nuevas necesidades tecnológicas armamentistas que requieran de los servicios del complejo militar industrial.

Por ello, es necesario llenar el vacío legal que ha producido la aparición de las EMSP: tanto estas empresas como sus trabajadores están libres de cualquier control jurídico y democrático en sus actuaciones, al mismo tiempo que están quedando impunes sus actuaciones por violación de los derechos humanos y el derecho humanitario. Es responsabilidad de los gobiernos controlar el impacto en las sociedades de esta industria y, para ello, es necesario que se desarrolle un marco regulador claro, riguroso y contundente, un marco que confiera transparencia en el proceso de contratación y en el establecimiento de procesos de seguimiento en el desarrollo operacional y financiero del contrato. Pero hay que tener presente que una industria globalizada requiere de una respuesta reguladora globalizada y, por tanto, dentro del marco de Naciones Unidas.

La robótica nos abre un escenario de futuro en donde las guerras se llevarán a cabo mediante las máquinas. Es muy improbable que las armas totalmente autónomas o los llamados robots autónomos letales puedan llegar a alcanzar las cualidades humanas necesarias para respetar las normas del Derecho Internacional Humanitario en materia de responsabilidad, distinción y proporcionalidad. Tampoco es creíble que los robots letales puedan llegar a tener cualidades humanas, que puedan llegar a tener la capacidad de relacionarse con los humanos como si fueran humanos, ni que lleguen a entender las intuiciones humanas o a procesar situaciones complejas y cambiantes. Igualmente, no se puede creer que lleguen a poder utilizar y aplicar el juicio humano y a afrontar situaciones subjetivas. Si los algoritmos de programación de los robots autónomos no pueden asegurar los principios del Derecho Internacional Humanitario ni la Convención de Ginebra dichas armas han de ser declaradas ilegales.

Un robot nunca se identificará con sus víctimas, nunca sentirá emociones, por ello usar robots autónomos letales en el ejercicio del uso de la fuerza, es hacer la guerra más inhumana. Finalmente, decir que tomar decisiones sobre la vida o la muerte de las personas tiene que quedar en manos de humanos, no de máquinas. La característica más humana que tenemos es la libertad de decidir nuestro destino, aunque tomenos la decisión incorrecta.

EXPERIENCIAS

Prácticas y respuestas en una sociedad vigilada

Lucía Vicent
FUHEM Ecosocial

Foto: Proyecto Remote Control

Desde el surgimiento de las sociedades han existido distintas técnicas de control y vigilancia de unos grupos hacia otros, donde la clase social ha estado más o menos presente en la configuración de los mismos. Más novedosas, sin embargo, son las formas concretas que hoy adquieren, y el nivel de concentración y omnipresencia de la vigilancia en manos de unos pocos.

Cada vez más institucionalizada, la vigilancia se confirma como un monopolio exclusivo de un sector de la sociedad, el de la clase capitalista, los dueños de los medios de producción. Al desarrollo tecnológico se le ha hecho concurrir con las inercias y los propósitos de la dinámica capitalista, a través de nuevas prácticas de acceso a la información o el desarrollo de nuevos sistemas de vigilancia, todos ellos necesarios para garantizar la reproducción del capital y la perpetuación del sistema.

Los ojos que vigilan se multiplican, su alcance es mayor y detectarlos se complica cada vez más. En distintos ámbitos en los que desempeñamos nuestra vida cotidiana (escuela, casa, hospitales, etc.) se registran nuestros movimientos, acciones e informaciones diversas que nos sitúan en un lugar de riesgo ante cualquier paso en falso que se dirija hacia la homogeneización social pretendida.

En respuesta, han proliferado toda una serie de organizaciones, movimientos y colectivos que, por un lado, nos alertan de los avances que se producen en las formas de control y vigilancia, y por otro, denuncian los riesgos a los que nos exponemos. Asimismo, en los casos en los que es posible, también realizan importantes esfuerzos de visibilización de estas prácticas y desarrollan herramientas concretas que pueden contribuir a sortearlas.

Espionaje, conflictos armados y control institucional

En el pasado, las telecomunicaciones y la informática han permitido controlar a la población civil y detectar comportamientos de 'anomalía" –dicho de otra forma, contrarios a los objetivos de aquellos que los controlan– con instrumentos y sistemas, hoy obsoletos, que se han modernizado hasta convertirse en sofisticados mecanismos que han ampliado el potencial de vigilancia y actuación sobre las sociedades. La primera vez que la población escuchó el término de vigilancia electrónica fue cuando se desveló la existencia de Echelon, la primera red de espionaje de la Agencia de Seguridad Nacional estadounidense (NSA), surgida tras la II Guerra Mundial. A partir de ese momento, no dejaron de aparecer descendientes con características bastante similares: Enforcement Police (ENFOPOL), el Sistema Integrado de Interceptación de Telecomunicaciones (SITEL) o el Sistema Integrado de Gestión Operativa, Análisis y Seguridad Ciudadana (SIGO) configuran otros ejemplos de espionaje y acceso de información privada a través de la intercepción de todo tipo de comunicaciones internacionales.

Desde su fundación en 1991, la organización sin ánimo de lucro conocida como Statewatch monitorea a los Estados y las libertades civiles que brinda cada uno en los países de la Unión Europea. A través de documentos periodísticos y artículos de investigación, sus integrantes abordan temáticas como la justicia, libertad de información, protección de datos, la rendición de cuentas, transparencia pública en las áreas comunitarias o los Derechos Humanos. Abogados, académicos, periodistas, investigadores y activistas de más de 14 países forman parte de esta red y concentran sus esfuerzos en la elaboración y difusión de los materiales que realizan.

El proyecto Remote Control se enmarca dentro Network for Social Change, una red que proporciona financiación a iniciativas orientadas hacia el cambio social, en concreto, aquellas relacionadas con cuestiones de paz, justicia o medio ambiente. Este proyecto surge en el año 2013 con el propósito de analizar la evolución actual de la tecnología militar y de cómo el replanteamiento de sus actuaciones pueda tener consecuencias muy graves para la sociedad, hasta el punto de señalarse como una de las principales amenaza para el futuro. Además de la una fuerte apuesta por la creación de conocimiento en esta temática, Remote Control es un instrumento para el intercambio de información y materiales realizados en este campo.

Asimismo, el Oxford Research Group (ORG) da eco a los materiales que genera Remote Control y complementa algunas líneas temáticas que se enmarcan dentro del control social y la seguridad a nivel mundial. Este think tank independiente lleva más de 30 años promulgando enfoques orientados hacia la sostenibilidad mundial como la alternativa a la confrontación violenta y a los conflictos globales. El desarrollo de la "seguridad sostenible" a largo plazo para todos significa comprender las causas profundas de los conflictos, y promover el diálogo y no la confrontación como el medio para un mundo verdaderamente seguro. Combinan conocimiento en profundidad y experiencia en el análisis, el diálogo y la propuesta sobre cuestiones de seguridad.

En 1999, como resultado del trabajo previo desarrollado por la Campaña Contra el Comercio de Armas (C3A), surge el Centre d'Estudis per la Pau J.M. Delàs, de Justícia i Pau, con la misión de fomentar una cultura de paz y construir una sociedad sin armas. Funciona como un centro de investigación y documentación sobre temas relacionados con los efectos perversos de las armas y el militarismo, el desarme y la paz. Combina el trabajo de estudio y publicación y colabora con otras agrupaciones como Stockholm Internacional Peace Research Institute (SIPRI), European Network Against Arms Trade (ENAAT), la Asociación Española de Investigación para la Paz (AIPAZ) y la Universidad Internacional por la Paz de Sant Cugat.

En esta misma línea, preocupados por la ética en la tecnología robótica, las relaciones internacionales, la seguridad internacional, el derecho internacional humanitario y por los peligros que los robots militares representan para la paz y la seguridad internacional y la población, trabajan otras muchas organizaciones sensibles a estas cuestiones. Algunos ejemplos los podemos encontrar en: International Commitee for Robot Arms Control (ICRAC), Human Rights Watch, Stop Killer Robots Canada o Women's International League for Peace and Freedom. Todas ellas se han sumado a la campaña en contra de los desarrollos robóticos usados en conflictos armados conocida como Stop Killers Robot.

Otras organizaciones amplían la denuncia de desarrollos tecnológicos con uso violento entre países. La organización Article 36 hace referencia al artículo del Protocolo I de 1977 adicional a los Convenios de Ginebra que exige a los Estados a revisar las armas, medios y métodos de guerra con el objetivo de prevenir daños no intencionados. Con sede en Reino Unido, esta organización sin fines de lucro trabaja en la denuncia y la lucha contra el daño involuntario, innecesario e inaceptable causado por las armas tradicionales y nuevas modalidades que se desarrollan como: los Killer robots (o 'robot de combate"), municiones de racimo, etc. A través de las actividades de investigación, acciones políticas y otras vías que utilizan tratan de establecer alianzas fuertes que respondan al uso de las armas y eviten daños mayores que los avances que se suceden originarán.

Las Tecnologías de Información y Comunicación (TIC) y la vigilancia en internet

El progreso tecnológico no siempre significa una mejora para el interés común de la ciudadanía. Sin salvaguardias democráticas que limiten el control de minorías elitistas sobre la aplicación de la tecnología, que impidan un ejercicio de poder ligado a sus intereses particulares, la potencialidad de los avances se puede convertir en importantes riesgos para la población.

La potencia de la tecnología y la extensión de su uso cotidiano nos alertan de que podemos vivir en sociedades de tintes orwellianos donde el interés colectivo se supedita al de unos pocos sin sentir tal imposición. La infinidad de datos personales capaces de recoger por la potencia de los actuales sistemas informáticos, a día de hoy, permiten identificar perfiles, estimar desviaciones e incluso hacer previsiones del comportamiento humano. A todas estas posibles aplicaciones de la información se las conoce como 'Big Data". Su aplicación se extiende principalmente a través de grandes empresas, con vistas a mejorar sus beneficios, o Estados que, bajo el argumento de la seguridad ciudadana, amplían sus márgenes de control sobre la población y abren nuevas vías para trasladar sus intereses.

Existen organizaciones que defienden y luchan por extender los derechos digitales de todos los usuarios, en especial los de aquellas personas que pueden verse en mayor medida comprometidos (activistas, movimientos sociales, etc.). Un ejemplo lo encontramos en Access que, mediante la combinación de políticas innovadoras, participación de los usuarios, y el apoyo técnico, luchan por las comunicaciones abiertas y seguras para toda la población. Sus integrantes entienden que la tecnología puede ser una poderosa plataforma que facilita una mayor participación, la rendición de cuentas y la transparencia (cuestiones que tratan en las campañas que realizan) pero nunca puede suponer riesgos adicionales para la seguridad de los usuarios.

La Electronic Frontier Foundation (EFF) es una de las agrupaciones principales en la defensa de las libertades civiles en el mundo digital. Fundada en 1990, defiende la privacidad de los usuarios, la libre expresión y la innovación y lo hace a través del análisis de las políticas que se desarrollan en estas competencias y el activismo de base que refuerza y protege los derechos y libertades en el uso tecnológico. Son muchas las campañas que realizan para lograr su propósito, entre las que podemos destacar las de mayor actualidad: Stop TPP Fast Track, que denuncia la posible aplicación de derechos de propiedad intelectual más restrictiva en el marco del Acuerdo Transpacífico que se está negociando, o la iniciativa Oppose NSA Mass Spying!, en contra de que el Gobierno de EEUU, junto con la ayuda de las principales operadoras de telecomunicaciones, ejerza una vigilancia ilegal y masiva a través de las comunicaciones.

Originalmente, Proyecto Tor (o Tor Project) fue desarrollado por la Marina estadounidense con el objetivo de proteger las comunicaciones gubernamentales. Sin embargo, hoy en día, es utilizado de forma habitual por gente normal, periodistas, activistas y muchos otros con fines de privacidad. La red supone una estructura de túneles virtuales que mejora la seguridad de la información que intercambiamos a través de internet, además de permitir desarrollar aplicaciones con herramientas de privacidad incorporadas que impiden el seguimiento de sitios webs. El uso de Tor protege contra una forma habitual de vigilancia en internet conocida como "análisis de tráfico", que puede interceptar quién está hablando a quién en una red pública. Muy utilizado por periodistas en sus comunicaciones con confidentes y disidentes o entre personas que han sido víctimas de agresiones, entre otras muchas personas.

Un control ciudadano que compromete derechos fundamentales

Las diferencias existentes en el uso de las nuevas tecnologías son muy diferentes entre unos lugares y otros, con mayores libertades y derechos en algunos, y más restrictivos en otros. No nos referimos solo a los que tienen que ver con internet y la protección de datos, las restricciones y formas de control social avanzan en otras muchas direcciones. Un buen punto de partida para saber en qué contexto nos movemos en cada caso es en el que nos sitúa, gracias a la información que nos facilita, el Observatorio Latinoamericano de Regulación, Medios y Convergencia u OBSERVACOM. Esta iniciativa creada por expertos e investigadores de la comunicación se centra en el monitoreo sistemático del desarrollo de marcos normativos y políticas públicas de comunicación con la finalidad de producir análisis e informaciones que permitan evaluar su impacto en la libertad de expresión, la diversidad y el pluralismo en los sistemas de medios de la región.

La invalidación, por parte del Tribunal de Justicia de la Unión Europea (TJUE), de la directiva que obligaba a los operadores de telecomunicaciones a conservar datos de los usuarios durante dos años. Considerada como una injerencia grave en dos derechos fundamentales: el respeto de la vida privada y la protección de datos personales.

Una palabra, una foto o una imagen pueden poner en riesgo la libertad y la vida de una persona en ciertos lugares del mundo. Ciertos poderes que campan a sus anchas en puntos concretos del globo, pueden impedir –y así lo hacen– que ciertas informaciones en las que, o bien pueden verse envueltos, o bien les beneficia que sigan ocurriendo, salgan a la luz. Reporteros sin Fronteras (RsF) desde 1985 trabaja para que esto no siga ocurriendo. Por la defensa de la libertad de prensa, porque encarcelar a un periodista es eliminar a un testigo esencial y amenazar el derecho de todos a la información, por esos y otros motivos, RsF defiende a todos aquellos colaboradores de los medios de comunicación que puedan verse perseguidos por desarrollar su actividad

profesional. Entre otras actividades, es reseñable el barómetro que la agrupación muestra en su web (con el número de casos de periodistas o internautas encarcelados o asesinados), la campaña de apadrinamiento, la clasificación mundial de la libertad de prensa o los informes sobre los 'enemigos de internet".

En la misma línea se mueve Global Voices Advocacy, una red global de *bloggers* y activistas dedicados a la protección de la libertad de expresión y el libre acceso a la información en línea. Este proyecto se enmarca en Global Voices Online. Entre otras de sus actividades, informan sobre las amenazas de la libertad de expresión, comparten estrategias para defenderse y apoyan los esfuerzos para mejorar las políticas y las prácticas en Internet.

El derecho a la libertad de expresión y el acceso a la información no son los únicos que se restringen con el avance del control y la vigilancia por parte de las instituciones, sino que existen otros muchos, como ocurre con el de la defensa. Cada vez son más las abogadas y abogados que por ejercer la defensa de los ciudadanos de forma independiente con el propósito de alcanzar la máxima democratización en esta competencia, se sienten amenazados, perseguidos o coaccionados. Desde la Asociación Libre de Abogados (ALA) de Madrid se lucha contra las limitaciones que las autoridades públicas en muchas ocasiones establecen en la defensa de la ciudadanía. Para ello, cuentan con distintos mecanismos: misivas a embajadas, autoridades públicas y Defensorías del Pueblo; comunicaciones y quejas a autoridades y comisiones internacionales; llamamientos on-line a la sociedad civil; convocatoria y participación en actos públicos; concentraciones de protesta, intercambio de información con otras organizaciones jurídicas y de derechos humanos, etc.

Muchas de las reformas que aprueban las instituciones promueven la intensificación de las prácticas de control y vigilancia ciudadana. Así lo denuncian distintos colectivos y agrupaciones como la plataforma No Somos Delito que está integrada a su vez por más de 70 organizaciones unidas contra los pasos legislativos que se suceden que coartan las libertades civiles y derechos de las personas en materia de seguridad y protesta social. Algunos ejemplos de denuncia podemos encontrarlos en: la oposición a la Ley mordaza o a las novedades del nuevo Código Penal así como en el análisis del proyecto de Ley de Seguridad Ciudadana.

En paralelo a la denuncia de los cambios regulatorios, son muchos los colectivos y grupos sociales que promueven acciones para la defensa de los derechos básicos y ciudadanos. En nuestro país, uno de los máximos referentes son las Brigadas Vecinales de Observación de Derechos Humanos, organizadas en Madrid para visibilizar y denunciar los controles policiales y redadas masivas a migrantes que se suceden. En concreto, sus focos de atención son los controles de frontera que se realizan en lugares estratégicos de uso cotidiano en función de la apariencia, las redadas policiales que

criminalizan la libertad de movimiento de las personas procedentes de países de la periferia económica, o los requisitos prácticamente imposibles de cumplir que exigen a las personas inmigrantes para otorgarles los permisos de residencia y trabajo.

SELECCIÓN DE RECURSOS

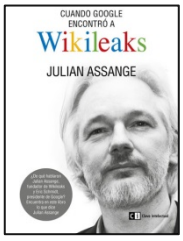
Estado de excepción y control social

Susana Fernández Herrero
FUHEM Ecosocial

Libros

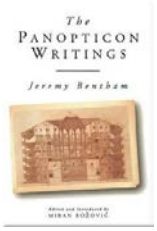
ALCÁNTARA, José F., *La sociedad de control: privacidad, propiedad intelectual y futuro de la libertad*
Ed. El Cobre, 2008.
Texto completo

ASSANGE, Julian, *Cuando Google encontró a Wikileaks*
Madrid: Clave intelectual, 2014.
Entrevista de Ignacio Ramonet

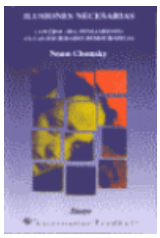


BELIL Mireia, Jordi Borja y **Marcelo Corti** (eds.),
Ciudades. Una ecuación imposible
Barcelona: Icaria, 2012.
Reseña

BENTHAM, Jeremy, **Miran Bozovic** (ed.)
The Panopticon Writtings
Londres: Verso, 1995.

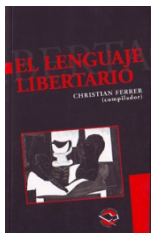


BRANDARIZ, José Ángel; **Jaime Pastor** (eds.),
Guerra global permanente: la nueva cultura de la inseguridad
Madrid: Catarata, 2005.
Resumen



CHOMSKY, Noam, *Ilusiones necesarias.*
Control del pensamiento en las sociedades democráticas
Madrid: Libertarias, 1992.
Reseña

DELEUZE, Gilles, 'Posdata sobre las sociedades de control",
en **FERRE, Christian** (ed.), *El lenguaje libertario. Antología al pensamiento anarquista contemporáneo*
Buenos Aires: Altamira, 2000.
Artículo

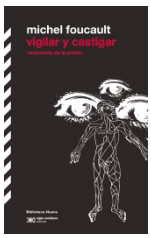


DELGADO, Manuel, *El espacio público como ideología*,
Madrid: Catarata, 2011.
Reseña

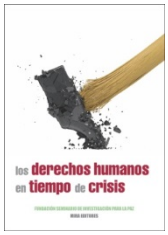
FERNÁNDEZ BESSA, Cristina; **Héctor Silveira Gorski**, **Gabriela Rodríguez Fernández**, **Iñaki Rivera Beiras** (eds.),
Contornos bélicos del Estado Securitario: control de la vida y procesos de exclusión social,
Barcelona: Anthropos, 2010.
Información

FLEURY; Sonia; **Joan Subirats** e **Ismael Blanco** (eds.)
Respuestas locales a inseguridades globales: innovación y cambio en Brasil y España,
Barcelona: Fundación CIDOB, 2009.
Texto completo

FOESSEL, Michaël, *Estado de vigilancia: crítica de la razón securitaria*,
Madrid: Lengua de trapo, 2011
Información



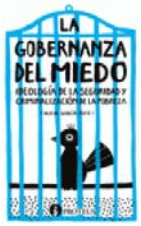
FOUCAULT, Michel, *Vigilar y castigar: nacimiento de la prisión*
Madrid: Siglo XXI, 2012
Reseña



FUNDACIÓN SEMINARIO DE INVESTIGACIÓN PARA LA PAZ, (SIP)
Los derechos humanos en tiempo de crisis
SIP, Zaragoza, 2014
Presentación

Capítulo 6: El derecho a la paz y la tendencia armamentística actual

- **Tica Font Gregori**, *El impacto de la creciente tendencia armamentística sobre los derechos humanos.*
- **José Luis Gómez del Prado**, *Las empresas militares y de seguridad privadas en los conflictos armados: sesgo preocupante para los derechos humanos*.
- **Javier Jiménez Olmos**, *La actual crisis social: señal de alerta para la seguridad humana e internacional.*



GARCÍA RUIZ, ALICIA, *La gobernanza del miedo: ideología de la seguridad y criminalización de la pobreza*
Barcelona: Proteus, 2013
Resumen

GARNIER, Jean Pierre, **'**Un espacio indefendible. La ordenación urbana en la hora securitaria", en *Contra los territorios de poder:*
por un espacio público de debates... y de combates
Barcelona. Virus, 2006, pp. 103-129
Texto completo

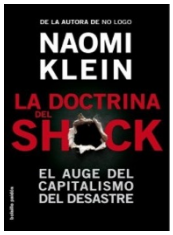
GIORGI, Alessandro de,
El gobierno de la excedencia: posfordismo y control de la multitud
Madrid: Traficantes de sueños, 2006
Texto completo

GONZÁLEZ ZORRILLA, Carlos, *¿Quién controla a los controladores? Policía, justicia y control democrático*
Barcelona: Base, 2013
Resumen

HERNÁNDEZ, Esteban, *El fin de la clase media*
Madrid: Clave intelectual, 2014.
Presentación

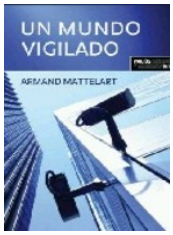
JACOBS, Jane, *Muerte y vida de las grandes ciudades*
Madrid: Capitán Swing, 2011
Reseña

JORDÁN, Javier; **Josep Baqués Quesada**,
Guerra de drones: política, tecnología y cambio social en los nuevos conflictos
Madrid. Biblioteca Nueva, 2014
Introducción



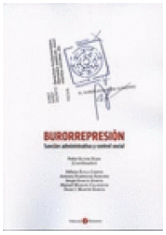
KLEIN, Naomi, *La doctrina del shock: el auge del capitalismo del desastre*,
Barcelona: Paidós, 2007.
Reseña

LESSIG, Lawrence, *Por una cultura libre: Cómo los grandes grupos de comunicación utilizan la tecnología y la ley para clausurar la cultura y controlar la creatividad*
Madrid: Traficantes de Sueños, 2005.
Texto completo



MATTELART, Armand, *Un mundo vigilado*
Barcelona. Paidós, 2009.
Reseña

MONTOYA, Roberto, *Drones: la muerte por control remoto*
Madrid: Akal, 2014.
Reseña



OLIVER OLMO, Pedro (coord.), *Burorrepresión: sanción administrativa y control social*
Albacete: Bomarzo, 2013.
Presentación

PISARRELLO, Gerardo; Jaume Asens, *La bestia sin bozal: en defensa del derecho a la protesta*
Madrid: Catarata, 2014.
Reseña

UGARTE, David de, *El poder de las redes: manual ilustrado para ciberactivistas*
Barcelona: El Cobre, 2007
Texto completo

VELASCO, Demetrio, *Fascismo social: políticas del miedo y servidumbre voluntaria ¿Qué hacer?*
Bilbao: Universidad de Deusto, 2013
Texto completo

Revistas

REVISTA PAPELES DE RELACIONES ECOSOCIALES Y CAMBIO GLOBAL

PAPELES de Relaciones Ecosociales y Cambio Global es una revista trimestral publicada desde 1985 por el área Ecosocial de FUHEM y coeditada con Icaria editorial.

Con una mirada interdisciplinar, la revista aborda temas relacionados con la sostenibilidad, la cohesión social y la democracia, considerando la paz como eje transversal de análisis. Papeles de Relaciones Ecosociales y Cambio Global es hoy una referencia indiscutible para conocer los principales problemas y debates de nuestro tiempo.

El pensamiento de analistas, teóricos y activistas, tanto del panorama nacional como internacional, hacen de las páginas de Papeles escenario intelectual crítico para una sociedad justa en un mundo habitable.

Selección de artículos

Jordi Borja, Ciudad, urbanismo y clases sociales en perspectiva, núm. 126, verano 2014, pp. 111-127

María Castrillo, Ángela Matesanz, Domingo Sánchez Fuentes y Álvaro Sevilla, ¿Regeneración urbana? Deconstrucción y reconstrucción de un concepto incuestionado, núm. 126, verano 2014, pp. 129-139.

Luis Carlos Nieto Garcia, Rompiendo las costuras de las garantías. Comentarios al anteproyecto de ley de seguridad ciudadana, núm. 124 invierno 2013-14, pp. 63-75.

Brigadas Vecinales, Brigadas Vecinales de Observación de Derechos Humanos contra los controles racistas en Madrid, núm. 124, invierno 2013-2014, pp. 103-110.

Tica Font y Pere Ortega, Seguridad nacional, seguridad multidimensional, seguridad humana, Papeles de relaciones ecosociales y cambio global, núm. 119, otoño 2012, pp. 161-172

María Naredo Molero, El miedo de las mujeres como instrumento del patriarcado. Claves para una política pública de seguridad ciudadana que incorpore las necesidades y demandas de las mujeres, núm. 109, primavera 2010, pp. 79-86.

Tanja Bastia, Urbanización, migración y exclusión social: viñetas desde las villas miseria, núm. 98, verano 2007., pp. 83-91

REVISTA RELACIONES INTERNACIONALES

Relaciones Internacionales se crea en el año 2004 por un grupo de alumnos y profesores del Programa de Doctorado "Relaciones Internacionales y Estudios Africanos" del Departamento de Ciencia Política y Relaciones Internacionales de la Facultad de Derecho de la Universidad Autónoma de Madrid.

Publicación en formato electrónico que busca fomentar el estudio y debate sobre cuestiones actuales de relaciones internacionales desde un enfoque interdisciplinar y siempre vertebrado por tres ejes: teoría, historia y análisis. Uno de los principales objetivos con los que se iniciaba el proyecto era y es traducir a lengua castellana aquellos textos considerados como clásicos por los especialistas, con el fin de proporcionar herramientas a la comunidad académica de habla hispana que enriquezcan la reflexión sobre las relaciones internacionales. Aunque cada uno de sus números gira en torno a un tema específico, no se trata de monográficos. El objetivo es proporcionar contenidos que ofrezcan diversos enfoques y análisis sobre un tema propuesto que domina el número pero reservando siempre un porcentaje de los contenidos a textos que abordan otros temas.

Crisis, seguridad, política, núm. 23, junio-septiembre 2013

Crisis, Seguridad, Política, pp. 5-13

Marcos Aurelio Guedes de Oliveira y **Carlos Federico Domínguez Ávila**, *El legado de Westfalia y la emergencia del postwesfalianismo en la seguridad regional de América del Sur*, 15-33.

Mariano César Bartolomé, *Una visión de América Latina desde la perspectiva de la agenda de la Seguridad Internacional contemporánea, 35-64.*

Fabrice Argounés, *Mitologías australianas contemporáneas: comunidad, seguridad, alteridad, territorialidad*, 65-80

Angie A. Larenas Álvarez, *La confluencia entre estudios críticos de seguridad y seguridad humana: las dinámicas de inclusión y superación,* 81-98

Fragmentos
Ken Booth, *Seguridad y emancipación*, 99-116

Andreas Behnke, *El Terror y lo Político: el 11-S en el contexto de la globalización de la violencia*, 117-148.

Ventana Social
La revuelta siria y sus retos para los discursos de seguridad actuales Entrevista a Sirin Adlibi Sibai, 149-154

Paolo Cossarini, *Deconstruir la seguridad: relaciones internacionales y pensamiento Político,* 155-162.

REVISTA PAPERS

'Papers' es una revista publicada por el Instituto de Estudios Regionales y Metropolitanos de Barcelona. La Colección tiene como objetivo hacer llegar el debate sobre los problemas y opciones de la Región Metropolitana de Barcelona, que hoy se encuentra en una fase decisiva de su evolución, a un amplio sector de personas e instituciones interesadas en el devenir de este territorio. El contenido de 'Papers' incluye desde aportaciones de expertos o resúmenes de trabajos directamente motivados por esta temática hasta textos y compilaciones de datos de distinta procedencia que tienen un estimable valor de referencia.

La revista incluye los artículos en catalán, y su traducción al inglés y al castellano (a partir de la página 81.

La seguridad ciudadana en las metrópolis del siglo XXI, Papers, núm. 53, enero 2011.

LA SEGURIDAD CIUDADANA
Jaume Curbet, *La inseguridad ciudadana ha cambiado nuestras vidas*, 81-86.

LA GESTIÓN DE LA SEGURIDAD CIUDADANA

Francesc Guillén Lasierra, ***Las políticas de seguridad ciudadana***, 86-92.

LA SEGURIDAD CIUDADANA EN ALGUNA METRÓPOLIS DE EUROPA Y AMÉRICA DEL NORTE

Marcel Cajelait, *La seguridad en Montreal, un resultado colectivo*, 93-96.

James Bennett, Betsy Stanko, *La seguridad ciudadana en el Londres del siglo XXI*, 96-101.

Christophe Soullez, Alain Bauer, *La Seguridad ciudadana en grandes aglomeraciones francesas*, 101-106.

Carles González Murciano, Marta Murrià Sangenís, *La seguridad desde una perspectiva metropolitana. El caso de Barcelona*, 106-109.

REVISTA TEKNOKULTURA

Teknokultura: Revista de Cultura Digital y Movimientos Sociales se resiste a la asimilación de los estudios sociales de la tecnología y la cibercultura por sectores hegemónicos y, por tanto, a que se relegue a grupos y colectivos que apuestan por modos distintos de producción y colectivización del capital cultural. Al igual que un laboratorio de experimentación – hacklab – , Teknokultura reúne esfuerzos colectivos con el propósito de profundizar en contenciosos tecnosociales, posicionarse ante los mismos e incitar "participaciones aumentadas".


Teknokultura. Revista de Cultura Digital y Movimientos Sociales

Vol 11, No 2 (2014): Vigilancia global y formas de resistencia

Tabla de contenidos

Karpeta

Vigilancia global y formas de resistencia, vol. 11, núm. 2, julio- agosto 2014.

Javier de Rivera, Ángel Gordo López, Vigilancia global y formas de resistencia, 237-242

Alejandro Segura Vázquez, *El pastor, el doctor y el Big Data*, 243-257.

Paola Ricaurte Quijano, Jacobo Nájera Valdez, Jesús Robles Maloof, *Sociedades de control: tecnovigilancia de Estado y resistencia civil en México*, 259-282

Santiago Ruiz Chasco, *Videovigilancia en el centro de Madrid. ¿hacia el panóptico electrónico?*, 301-327.

Gemma Galdon Clavell, *¿La vigilancia vestida de seda? Hacia una comprensión de la contra-vigilancia como discurso y práctica crítica*, 329-348

Sophia Carmen Vackimes, *Ensamblajes de vigilancia viajera*, 283-300.

Paloma González Díaz, *Reacciones en el Media Art ante la vigilancia y el control de datos en laRed: nuevos paradigmas (2001-2010).* 349-382.

Rafael Dernbach, Hackeando la máquina visual: la deconstrucción de las imágenes de control en las obras de Farocki y Paglen, 283-403

Héctor Puente Bienvenido, Costán Sequeiros Bruna *Poder y vigilancia en los videojuegos*, 405-423

A des/propósito de…

Ashlin James Lee, *Una cuestión de Momentum Reflexiones críticas sobre las opciones individuales de resistencia a la vigilancia*. 425-440

Jorge Dueñas Villamiel *Del camuflaje en el arte contemporáneo a la privacidad en el Net-Art*, 441-452.

Julia Varela Fernández, Fernando Álvarez-Uría, Hélène Castel *Entrevista a Hèlène Castel, autora de Retour d´exil d´une femme recherchée (2009), 453-473.*

REVISTA VIENTO SUR

VIENTO SUR es una revista política que se edita con periodicidad bimestral desde 1991. Tiene como referencia un marxismo abierto, crítico y autocrítico, que necesita y busca la comunicación y el encuentro con otras corrientes del pensamiento emancipatorio, especialmente aquellas directamente vinculadas con los movimientos sociales.

VIENTO SUR está comprometida en la lucha contra el capitalismo y solidaria con todas las personas y organizaciones que participan en ella. En sus páginas se encuentran informes, opiniones y debates de diferentes corrientes de la izquierda alternativa y de los movimientos sociales.

Crisis urbanas y derecho a la ciudad, núm. 116, mayo 2011.

Crisis urbana y derecho a la ciudad

Carlos Sevilla Alonso, Presentación, pp. 31-33

Henri Lefebvre, *Metamorfosis planetarias*, pp.35-38

Jordi Borja, *Espacio público y derecho a la ciudad*, pp. 39-49

Emmanuel Rodríguez, Isidro López, ***Circuitos secundarios de acumulación y competitividad territorial***, pp. 49-57.

Ibán Díaz y Cristina Honorato, *El urbanismo del miedo y la sociedad contemporánea*, pp. 58-67

Grupo Surrealista de Madrid, *El barón Hausmann sube a los cielos*, pp. 67-73.

Paco Segura, *Luchas ciudadanas por unas zonas metropolitanas habitables*, pp. 80-87.

Antonio García, *De la "V de vivienda" a los afectados por la hipoteca: la vivienda como objeto de batalla*, pp. 88-94.

Carlos Sevilla Alonso, *Tecnópolis y ciudades-empresa ¿Privatopías empresariales metropolitanas?*, pp. 95-102.

Miguel Romero, *Sobre todo, sin miedo. Entrevista a Rita, Fabio, Andrea y Pablo de Juventud sin Futuro*, pp. 109-118.

Miguel Romero, *Ramón Fernández Durán (1947-2011)*, pp. 119-121.

Aurora Justo, *Transformaciones en el barrio de Malasaña. Hacia la gentrificación*, pp. 73-79.

VAGUARDIA DOSSIER

Esta publicación trimestral del Grupo Godó desarrolla un tema internacional de forma monográfica. Especialistas internacionales de prestigio dan las claves para comprender el mundo.

La Ciberguerra, núm. 54, enero/marzo 2015

Álex Rodríguez , *Ciber: guerra, ataque, espacio, disuasión…* , p. 3

Walker Laqueur, *La guerra cibernética ('juegos de guerra')*, pp.6-15

UNA CRONOLOGÍA DEL CIBERCONFLICTO, pp. 16-17

Daniel Ventre, *Aparición de la ciberguerra: evolución de la guerra desde hace un siglo*, pp.18-25

Timothy Edgar, *¿Modifican las armas cibernéticas las leyes sobre la guerra?*, pp. 27-31

Dmitry (Dima) Adamsky, *Disuasión y ciberespacio*, pp.33-37

Stefano Mele, *La batalla por el ciberespacio y las armas cibernéticas*, pp. 38-41

Peter Warren Singer, *Ciberarmas y carreras de armamentos: un análisis*, pp. 43-44

RADIOGRAFÍA DE UN CIBERATAQUE, pp. 45-47

Jeffrey Carr, *La capacidad de guerra cibernética de un país*, pp.48-59

Scott Borg, *No es una guerra fría*, pp. 61-67

Eric Filiol, *La realidad operacional de la ciberguerra y de los ciberataques: cómo paralizar un país*, pp. 69-73

DEL SÍLEX AL GUSANO (LAS ARMAS A TRAVÉS DEL TIEMPO), pp. 74-77

Tiffany Strauchs Rad, *Hackers: antiguos enemigos, nuevos aliados*, pp. 79-81

c/ Duque de Sesto, 40
28009 – Madrid
Tel. +34 914 310 280
ecosocial@fuhem.es
www.fuhem.es/ecosocial