

APUNTES CONTRA EL MUNDO SMART, CONTRA LA NO-VIDA...



Barcelona, noviembre de 2017

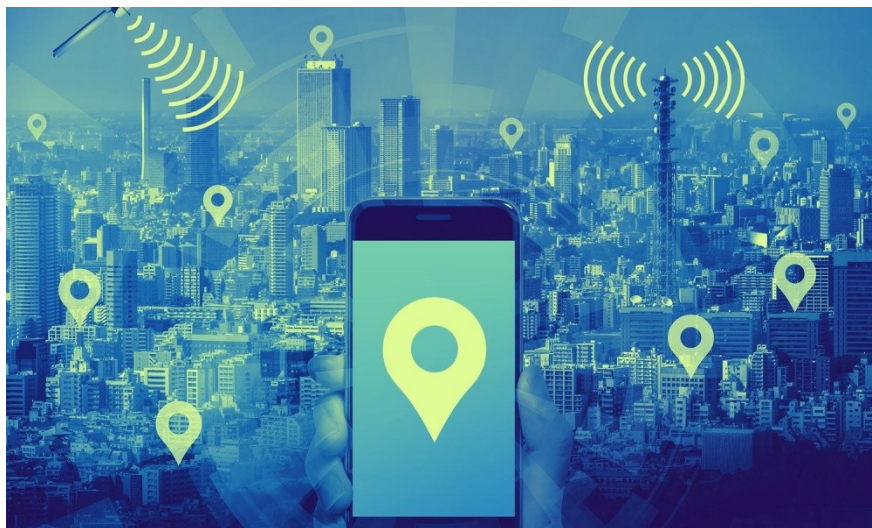
VIVIR, TRABAJAR Y SOBREVIVIR EN UNA SMART CITY.

El término “smart city” tiene sin duda una definición coyuntural, es un término “comodín” como lo han sido otros términos, por ejemplo la interculturalidad o la sostenibilidad. Sin embargo, que tenga un uso de velo ideológico o de cortina de humo no nos ha de impedir ver otras implicaciones. El término es difícilmente separable de otros como “internet de las cosas” o “bigdata”... aunque los “expertos” pretenden diferenciarlos totalmente. Ponerle un nombre a algo no es un acto neutro, el uso de las palabras tiene muchas más implicaciones de las que se pretenden y se relaciona muy directamente con el ejercicio del poder.

De hecho, lo que se esconde detrás de las “Smart city” no es nada diferente sustancialmente de la “vieja dominación”, sólo que ahora con instrumentos mucho más eficaces y potentes a su disposición. A la hora de hablar de Smart city no hay que perder de vista esto, el núcleo duro, lo importante, no es la cobertura tecnológica, sino la dominación de las corporaciones y los estados sobre las personas, los animales y el mundo.

La Smart city supone una tecnificación del viejo control social: en lugar de estar controlados por los chafarderos y los confidentes del barrio (los sensores) lo estamos por sensores (chafarderos y confidentes).

El que lo diferencia de los antiguos métodos es su extensión, profundidad y magnitud de sus bases de datos, así como la velocidad de proceso, la capacidad de almacenamiento, la rebaja brutal de los costes de todo este control y, finalmente, la posibilidad, cada vez más extendida, de control en tiempo real.



En el período 2013/2014, se han puesto en el mercado 7,700 millones de sensores Smart y 250 millones de tarjetas NFC. A estos hay que añadir los teléfonos inteligentes, las tablets y otros dispositivos conectados que, en la práctica, actúan como sensores y que a lo largo del período 2009/2014 han sobrepasado largamente los 10.600 millones de unidades. Se calcula que una ciudad con un millón de habitantes tenía en el 2010 unos 600.000 sensores, esta cifra, actualmente se

sobrepasa de largo.

Cisco y Eriksson han hecho una proyección para 2020 en que hablan de 50 millardos (billones americanos) de sensores y aparatos conectados. Se trata de una estimación a 6 años vista, pero nos da una idea de la magnitud de la futura recolección de datos. Otras estimaciones más conservadoras, hablan de 25 o de 35 millardos.

De todos modos, teniendo en cuenta que la población mundial en 2020 se estima que será de 7.717 millones de personas, tenemos un abanico de entre 3,2 y 6,5 dispositivos por habitante (los cálculos de Cisco y Eriksson no incluyen smartphones ni tabletas, ni los diferentes tipos de ordenador).

El objetivo básico de todos los proyectos de Smart city es la recogida de datos, unos para almacenarlos y tratarlos posteriormente (bigdata) y otros para decidir a tiempo real. Los usuarios son básicamente los intereses económicos detrás de los estudios de mercado, los diferentes tipos de policía y agencias de seguridad, los servicios de recursos humanos...

VIVIR EN UNA SMART CITY.

Nuestra vida cotidiana, ahora mismo, ya está muy penetrada por el seguimiento Smart. Dejando aparte el tema de los aparatos móviles (básicamente teléfonos), hay centenares de videocámaras que nos vigilan en los espacios públicos.

La videovigilancia, con la disminución del costo de grabación y almacenamiento de los datos, se está extendiendo y se hace ubicua. Además con la “videovigilancia inteligente” cámaras digitales con un software interpretativo se puede extraer en tiempo real mucha información de la grabación: números de matrícula, cantidad de vehículos y de personas, algunos rasgos del comportamiento de las personas grabadas, reconocimiento facial, detección de conductas sospechosas e incluso determinados estados anímicos.

La videovigilancia se ha “democratizado”, se venden miles de cámaras acompañadas casi siempre de software para vigilar una tiendecita o el hogar, para controlar hurtos, empleados, canguros, niños, mascotas i ancianos. Casi siempre son aparatos adquiridos por internet i autoinstalados o instalados por el manitas del barrio, evidentemente no cumplen ninguna de las condiciones de la ley de protección de datos.

Estas cámaras que hace unos años eran casi de juguete han alcanzado el rango de herramientas sofisticadas de alta resolución, conectables vía wifi con internet y dotadas de un software complejo que permite configurarlas con alarmas a teléfono y ordenadores, capaces de diferenciar personas, acciones i situaciones y definir áreas de vigilancia. Este software és también relativamente económico y normalmente va acompañado de almacenamiento en la nube, o sea que las imágenes quedan fuera del control del mismo interesado (que seguramente será grabado también).

Podemos resumir que ahora padres, hijos... no ejercen de cuidadores, sinó de vigilantes, de vigilantes por cuenta del estado y de la “nube”...

Cada vez es más difícil hacer un pago “en efectivo” (anónimo), cada vez aumenta más el conocimiento de nuestros hábitos de consumo por parte de los vendedores, los estados y las corporaciones (que, cuando, en que cantidad...). Cada vez tenemos más tarjetas con un chip, más documentos de identificación electrónico...

En nuestros hogares, los smartmeters que últimamente se están generalizando permiten conocer lo más íntimo de nuestros hábitos: cuando llegamos, cuando vamos a dormir, cuando nos duchamos i cuando ponemos lavadoras... si tenemos visitantes, si tenemos picos de consumo...

Determinadas tecnologías como los wearables (sensores “vestibles” que miden tensión arterial, ritmo cardíaco, oxígeno en sangre...), dan otra vuelta a la tuerca de control. Con ellos ponemos en unas manos desconocidas datos tan íntimos como nuestro estado físico y nuestra salud y, si están geoposicionados, la transparencia físico/metabólico “voluntaria” es total y absoluta.

Los riesgos de la Smart city parecen verse lejanos en el tiempo y en el espacio. Nos hacen creer que la tecnología del control Smart se aplica sólo en remotos países dictatoriales, o en fronteras con África o Oriente, también alejadas (al menos imaginariamente), o limitadas a perseguir delincuentes repulsivos (pederastas o violadores) y trabajadores malcumplidores (delincuentes?).

El hecho es que las tecnologías que se utilizan en estos momentos en las fronteras, sean de identificación o de detección, se están empezando a utilizar para el control interno sin que nos demos cuenta, aunque sólo fuese por egoísmo deberíamos combatirlos. Se están construyendo nuevas fronteras en las calles, en las instituciones y en los puestos de trabajo, fronteras que cada vez serán más evidentes... hasta que ya no nos las dejen cruzar... entonces será difícil derribarlas.

TRABAJAR EN UNA SMART CITY.

Vemos como cada vez más, en los puestos de trabajo, sobretudo aquellas que antes eran llamadas “trabajos manuales” los patrones tienen a su disposición un mayor número de herramientas de control y abuso derivadas de las Smart tecnologías.

Todas estas herramientas de control se disfrazan con la “amable intención” de liberar a los trabajadores de trabajos pesados o inseguros, pero el hecho es que la presión extra sobre el tiempo de ejecución y frecuencia de las operaciones hace que, por ejemplo, aumenten los accidentes laborales. Otro mito que nos han imbuido es el “buen rollo” de las empresas TIC (tecnologías de la información y la comunicación) con sus trabajadores. Sin embargo, en el mundo TIC, igual que en el resto del ámbito laboral, aumenta la fractura salarial entre los “bien pagados” y el resto.

Seguramente los primeros en padecer la Smart city fueron los trabajadores del espacio público, los de la limpieza viaria y del mantenimiento urbano. Fueron viendo como en todos sus vehículos (hasta en los carritos de los barrenderos) se instalaban GPS's y se les dotaba de agendas electrónicas (tipo palm), actualmente sustituidas por teléfonos (que a menudo han de pagar) para poder vigilar su actividad y comunicar las alarmas de trabajos urgentes.

Después fue el sector del transporte, especialmente mensajeros y repartidores de mercancías. De nuevo los GPS's y aquellos miniordenadores denominados Psion (ahora sustituidos por tablets). Estos trabajadores han de conducir, repartir, facturar... y en todo momento la central (el patrono) tiene trazable la mercancía (paquetes, cartas... y trabajadores). De hecho los “expertos” empresariales consideran que el 90% de las entregas en el 2018 se harán mediante sistemas conectados vía web (Uber, eBay Now, Shu!t!, Deliv, Postmates, Instacart, Amazon, Alibaba).

El transporte público de pasajeros vino detrás. Los autobuses con GPS y otros gadgets tecno-smarts, han invadido las flotas, al su vez, los taxis han incorporado taxímetros inteligentes y las videocámaras se han hecho omnipresentes en estaciones, vagones de metros y ferrocarriles, autobuses...

La recogida de residuos viene a continuación, con el añadido de los sensores de medida del llenado de contenedores, que harán variables los recorridos, las frecuencias y por tanto los horarios y el calendario de trabajo.

La mayor parte de las mercancías, palets, contenedores y muchos envases individuales ya vienen marcados con etiquetas RFID e incluso dispositivos más sofisticados, son trazables y los inventarios son casi automáticos. El impacto sobre los empleados de almacén y los reponedores es directo.

Los oficinistas y otros trabajadores de “cuello blanco” ya trabajan en red desde hace tiempo y padecen los software de control que registran desde el número de pulsaciones en el teclado hasta la actividad en todo momento de la jornada y... la inactividad.

En los comercios y tiendas no se vigila ya solamente a los posibles “ladrones/consumidores”, la vigilancia se extiende a los trabajadores con cámaras enfocando cajas registradoras y espacios “no

públicos"... De hecho a partir de una sentencia contraria a los deseos de la patronal se está haciendo firmar una comunicación de que las grabaciones se podrán utilizar como prueba para sancionar a los trabajadores.

Y en todas partes el control de presencia y de identidad se sofisticaba y cada vez necesita menos del contacto, llegando en algunos casos a controlar no sólo la entrada y la salida del trabajo, sino también el lugar y el tiempo pasado en diferentes dependencias, estableciendo zonas prohibidas a menudo arbitrarias.

Hay aplicaciones Smart especialmente repulsivas, como la escoba para limpieza urbana con sensor de movimiento que registra el número de barridos a lo largo del día (conectada también a un GPS en el carrito o en la escoba misma), o la ropa de trabajo "interactiva" dotada de etiquetas RFID u otros artilugios de control de presencia.

Se va imponiendo un modelo de economía de "servicios móviles bajo demanda" (ODMS), en el que no se trabaja para un empleador, sino para una plataforma que gestiona las demandas de los clientes y el pago (como UBER, Airbnb, Homejoy, la Nevera Roja...), además las empresas suelen estar ubicadas muy lejos del sitio donde se produce realmente el servicio. Es trabajar con un algoritmo como jefe o encargado, con la diferencia que a un algoritmo, con la diferencia de que a un algoritmo no se le puede coger por el pescuezo y tampoco se le pueden pinchar las ruedas del coche, esto nos deshumaniza y de hecho nos reduce al papel de otro algoritmo, al papel de un Smart trabajador.

Las aplicaciones Smart sólo tienen un límite: lo retorcida que tengan la mente los ingenieros y tecnólogos, la codicia de los empresarios y el afán de control sobre la vida de los demás.

Cual es el efecto de todo esto sobre las condiciones de vida en el lugar de trabajo?:

El primer efecto es un control extremo que va más allá del "ojo del encargado" o el reloj de fichar. Se trata de un control en tiempo real, no sólo de hora en hora o de minuto a minuto, sino que ahora ya se llega al control de milisegundo en milisegundo... Esto hace que el patrón (aunque parezca que sea un término obsoleto, todos tenemos un patrón aunque sea un estado o una corporación transnacional) sepa que hacemos en todo momento durante la jornada laboral (y fuera de ella si nos "permite" llevamos el Smartphone corporativo) y si la empresa es responsable "socialmente" y dispone de mejoras como actividades culturales y deportivas subvencionadas, entonces también conoce incluso una buena parte del tiempo libre.

El segundo Smart-efecto, es la "optimización del tiempo" por parte de la empresa: los ritmos de trabajo se aceleran y los plazos se acortan. Por ejemplo en el número de entregas de mercancías de un trabajador de UPS, la longitud del itinerario de un trabajador de la limpieza viaria, o el número semanal de expedientes de un oficinista.

El tercer efecto es un aumento de la precarización del trabajo. Por un lado, el control global genera despidos y por otro, el control extremo permite monitorizar y tutelar el trabajo de manera que, en cada momento, el trabajador se vea forzado a hacer "lo que debe hacer"... lo que desea la empresa.

El cuarto efecto global, es que la dominación extrema a la que nos lleva la "smartificación" ataca nuestra identidad individual y tiene efectos sobre nuestra libertad, la calidad de nuestras vidas y nuestra salud, hundiéndonos en la tecno miseria, la humillación y la dominación. Nos lleva a una negación de nosotros mismos y a una afirmación de nuestros dominadores.

LAS SMART FRONTERAS Y LAS SMART CITIES, O ESTAS DENTRO O ESTAS FUERA.

Las fronteras no suelen ser límites geográficos o naturales, tampoco son un límite jurídico administrativo, las fronteras son herramientas que el poder utiliza para acumular más poder o para regular su ejercicio.

El control de las fronteras ha ido evolucionando según SUS necesidades, los antiguos y enojosos "peajes" para regular el paso de las mercancías se ha ido optimizando para permitir el paso rápido de

todo aquello que puede generar valor, así el número de contenedores que mueve un puerto, por ejemplo el de Barcelona, sería impensable sin toda la capa de tecnología de identificación, de inventario y sin los mecanismos sociales de los que se dispone ahora.

Una de las mercancías más costosas de regular, y, de momento, imprevisible ya que tiene iniciativa propia, es la mercancía humana (trabajadores y consumidores), así pues es preciso regular estos flujos intentando reducir la “iniciativa propia” de las personas.

Esta “regulación” puede ir desde los disparos de los guardas de frontera, hasta los sofisticados muros de contención (con sus puertas de paso controladas) construidos en todas las fronteras, como el que hay entre los EUA y México, entre Gaza e Israel i en las fronteras de Ceuta y Melilla en el Estado Español. Los mecanismos de control han pasado del humano (siempre imperfecto) al inhumano (que también incluye a policías y otros funcionarios), atiborrando los muros de contención de sensores, cámaras i cuchillas de diferentes tipos.

De esta manera se han perfeccionado los pasaportes, los más modernos (prácticamente todos) están provistos de “micro chip”, de etiquetas RFID... y toda la parafernalia de entrada, rayos X, detectores de metales, escáners, sensores del latido cardíaco es cada día más perfecta. Los visados de los países de Schengen recopilan datos biométricos de los solicitantes (los diez dedos de las manos i la cara... de momento), los sistemas de visados (VIS) conectan las oficinas diplomáticas y los puestos fronterizos de los estados miembros.

El poder (básicamente estados y corporaciones) ha levantado los muros, pero estos muros no cubren todas las fronteras (se necesitaría cerrar todas las playas) ni son totalmente eficaces.

En el Estado Español la vigilancia de fronteras recae sobretudo en la Guardia Civil (GC) y también en el Servicio de Vigilancia Aduanera (SVA), estos cuerpos disponen de un buen arsenal de vehículos aéreos, marinos y terrestres. Tienen el apoyo de sistemas de vigilancia aérea y por satélite... y disponen de una amplia gama de sensores de todo tipo.

Entre enero de 2013 y agosto de 2014, la GC ha invertido alrededor de 6,5 millones de euros. La mayor parte del presupuesto se ha destinado a cámaras térmicas (5,1 millones). A sensorizar las patrulleras se han destinado 0,5 millones y a aparatos de visión nocturna 0,3. El SVA, dependiente de Hacienda no ha tenido unos gastos tan grandes en gadgets tecnológicos así que sólo han adquirido, en el mismo período, dos sistemas optrónicos de visión térmica y de visión diurna, eso si, de los caros, un milloncillo.

Una buena parte del esfuerzo controlador de la UE se hace a través de FRONTEX, la agéncia de gestión de fronteras exteriores, con sede en Varsovia. Esta agencia está en alza, su presupuesto, desde su creación en 2005, a pasado de 6 a 90 millones en el 2013.

FRONTEX está muy penetrada por los lobbys de las empresas de seguridad (INDRA, Thales, EADS, Selex, BMW...) que participan tanto en el desarrollo y gestión con tecnología propia (software, redes de comunicación, sistemas de control), como participan en proyectos conjuntos con fondos y partenaires públicos. Por ejemplo el proyecto PERSEUS (INDRA y EADS...) 43 millones de euros, el SEABILLA (INDRA, SELEX, Thales...) de 15 millones, TALOS (TTI Norte y la israelí IAI) de 3,9 millones y finalmente OPEMAR (Thales, INDRA y Selex) con sólo 669.000 euros.

FRONTEX, que en total a consumido más de 250 millones parece ir tomando posiciones para ocupar el papel de controlador único de las fronteras exteriores que ahora tienen los estados, especialmente a través de EUROSUR (centrado en las fronteras del Sur). De toda manera la estructura presupuestaria de la UE y el secretismo de los eurócratas de la seguridad, hace muy difícil averiguar si los recursos de FRONTEX han sido solamente estos 250 millones y que no dispone de más financiación, mediante la Agencia Europea de Defensa a través de fondos destinados a la investigación, al estímulo económico o a la seguridad interior.

El control de fronteras deviene evidentemente un gran negocio, se calcula que solamente el sector biométrico, en sus usos militares y de control de fronteras, generó el 2012 unos ingresos de 5.800

millones y se prevén beneficios de unos 15.800 millones para 2121. En el momento en que India y China se incorporen plenamente a este mercado los beneficios pueden crecer exponencialmente. De hecho el 27% de las conexiones máquina/máquina (M2M, la conexión básica sensor/servidor de las Smart city) están en China y el 40% mundial de conexiones M2M están en Asia.

El truco está en cerrar las puertas para que no entren los de fuera, las puertas son en un único sentido. El paso posterior será no dejar salir tampoco a los de dentro (puerta cerrada). El último paso: controlarnos a todos, la jaula para los animales domésticos.

Las Smart fronteras son padecidas ahora mismo por una inmensa mayoría de la humanidad (todos aquellos que no son ciudadanos de los países de la OCDE), pero en un futuro cercano, todas estas técnicas ya refinadas y desarrolladas se podrán aplicar directamente a la seguridad interna, para los estados del sur y también (para nuestra seguridad) a los refractarios de los países del norte.

SOBREVIVIR EN UNA SMART CITY.

Seguramente una perspectiva como la que hemos dibujado (los 50 millones de conexiones) da lugar al pesimismo y al derrotismo más absoluto, y la distopía parece inevitable... Pues nada de esto!! Quizás mejor que sobrevivir sería mejor hablar de “resistir a la Smart city”, o aun mejor “destruir la Smart city”.

La dominación y el control que constituyen el núcleo de la Smart city se implanta fácilmente y tiene el camino allanado gracias a los deseos y necesidades que nos han (y nos hemos) creado.

Queremos saber exactamente el tiempo que falta para que llegue el autobús y no nos importa que esta información lleve emparejada el control y la presión sobre los conductores.

Queremos tener servicios al instante a precios de saldo, no nos queremos enterar de la precarización y sobreexplotación de los trabajadores, como es el caso de UBER.

Queremos pasar a toda pastilla por los peajes y no hacer colas delante de las máquinas del metro, queremos una cola corta en la frontera y que el médico acceda a nuestro historial sin demora...

Queremos teleasistencia, queremos servicios a domicilio, queremos pedirlos por la red y obtenerlos deprisa y a un precio sospechosamente bajo.

Queremos finalmente ser provistos de todos los dispositivos móviles que nos permitan disfrutar de todo ello, los impactos de su producción sobre el agua, la tierra, las plantas y la fauna (nosotros incluidos) quedan en un segundo plano.

Queremos realmente la “Smart City??

A pesar de que esta red pueda parecer omnipresente no es para nada omnipotente, entre otras cosas porque se alimenta a si misma (se retroalimenta) y si se neutralizan un número suficiente de nodos pasa a ser inoperativa, total o parcialmente.

En el mundo antigua (hace muy poco) era posible vivir sin la mayoría de las redes urbanas, se podía vivir sin suministro de agua o de energía, sin servicios sanitarios, sin cuerpos de seguridad... esto se ha demostrado en las diferentes situaciones de emergencia ocurridas en el inicio del siglo XXI.

En New Orleans la gente se supo organizar para sobrevivir, mientras que el estado sólo se preocupaba por detener el saqueo. Recogieron comida y agua, supieron distribuirlas con mucha equidad y supieron encontrar espacios de seguridad. Cuando las redes del estado les volvieron a capturar, las cosas empeoraron y, todavía ahora, no están “normalizadas” y la gente sigue viviendo en quasibarracas sin servicios mínimos.

En Gaza, con la mayor parte de las redes de servicio no operativas, con el esfuerzo individual de los trabajadores y el esfuerzo colectivo de la población, han podido resistir y continuar viviendo sin un

funcionamiento regular de estas superestructuras.

Lo mismo podemos decir de situaciones de enfrentamientos militares entre estados en Siria, Irak, Kurdistan... o de desastres “naturales” como el tsunami de las Filipinas... o más recientemente el terremoto de Nepal.

Ahora bien, podría el actual sistema capitalsita resistir una semana sin internet?, sin red de comunicaciones?... que valor tendría el dinero depositado en New York, en Barcelona, en Londres?... la respuesta es fácil, a la primera No y a la segunda NADA. De aquí surge otra pregunta diferente: es posible detener, hacer caer o neutralizar la red? La respuesta es, creemos, que sí.

Hay un problema de enfoque. Nosotros queremos resistir al sistema localizadamente, cada cosa en su lugar: la PAH frente a Caixa Catalunya, los antinucleares frente a ENDESA, los antifronteras frente los CIES, los adversarios de los transgénicos ante MONSANTO... y así todos buscamos nuestra posición y nuestro “target” correcto... ellos por el contrario están hiperconectados (el Obispado con ENDESA, ENDESA con los CIES, los CIES con MONSANTO, MONSANTO con la Generalitat, la Generalitat con el rector de la parroquia...) y se ríen de nuestros esfuerzos localizados, limitados y, a menudo, estériles.

Historicamente muchos de los movimientos de protesta de los oprimidos no se han autolimitado nunca tanto en el alcance de sus luchas como nos autolimitamos actualmente. Esta especialización es reciente.

En las revueltas locales de los siglos XIX y XX, los insurrectos, además de las reivindicaciones puntuales, el coste de la vida, las condiciones de trabajo, la oposición al quintado de mozos... invariablemente destruían, generalmente mediante el fuego, los archivos del registro de propiedad, del registro civil, los catastros (red de control estatal) y las instituciones de la Iglesia: conventos, iglesias, escuelas, registros parroquiales... (red de control ideológico).

Por ejemplo, los anarcosindicalistas del Berguedà no se limitaron a las condiciones de las minas o fábricas y por esto pudieron proclamar, durante unos días, el comunismo libertario global para toda la vida cotidiana de varias poblaciones.

Los piqueteros argentinos no se limitaron a manifestarse delante de la Casa Rosada, también cortaron carreteras y otras vías de comunicación sin un objetivo “local”, únicamente contra el paro!!, teniendo efecto sobre otros sectores (capitalistas) no estrictamente vinculados a su conflicto.

Las sufragistas inglesas de principios del siglo XX no restringían su lucha a atacar al parlamento o a los partidarios del apartheid de género; entendieron que el patriarcado (que era su verdadero objetivo) tenía otros tentáculos más accesibles a los que dañar. Así que durante los años 1912-13, y parte de 1914, destruyeron centenares de buzones de correo (el internet de entonces) sin preocuparse (al contrario que los seguidores de la ética Hacker) en los efectos sobre terceros, incendiaron edificios, cortaron líneas de teléfono y de telégrafo, y sabotearon la red de ferrocarriles (como podemos ver, atacaron todas las redes a su alcance).

En estos momentos, las redes son vulnerables si las atacamos guiándonos, no por la lógica que nos imponen (antinucleares/instituciones energéticas, antipatriarcales/ministerio de justicia, anti OMG/MONSANTO...), sino por la lógica de la hiperconectividad de nuestros dominadores, NO IMPORTA DONDE ACTUES!, ESTAN HIPERCONECTADOS, YA LES LLEGARÁ EL EFECTO!!.

Con esta lógica, se trascendería el problema de la coordinación entre grupos y movimientos. También trascendería la lógica de los dominadores, la de la represión. Puedes atacar, alterar, destruir en cualquier punto, puedes reivindicar estas acciones para cualquier causa... puedes estar seguro que generarás más perjuicios que si gastas recursos y un tiempo valioso intentando identificar el punto justo, el punto correcto... porqué este punto no existe, está en todas partes... ATACA LA RED!!.

Autors: negreverd@nodo50.org

FRONTERAS Y TECNOLOGÍA

Las fronteras no suelen ser límites geográficos o naturales, tampoco son únicamente un límite jurídico administrativo, las fronteras son herramientas que el poder utiliza para producir más poder o para regular el ejercicio de este.

El control fronterizo ha ido evolucionando según las necesidades de este poder, los antiguos y engorrosos peajes para regular el paso de mercancías se han ido optimizando para permitir el paso rápido de todo aquello que genera valor.

Una de las mercancías más costosas de regular, de momento te iniciativa propia, es la mercancía humana (productores y consumidores), así pues que hay que regular estos flujos intentando reducir la “iniciativa propia” de las personas.

Esta regulación puede ir desde el disparo de los guardas de frontera de no hace demasiado tiempo, hasta los sofisticados muros de contención (con sus puertas controladas) construidos en las fronteras entre los EE.UU. y México, de Palestina y de las fronteras ceutís y Melilla del estado Español. Los mecanismos de control han Pasado del control humano (siempre imperfecto) al inhumano (que también incluye policías y otros funcionarios) siempre en perfeccionamiento, siempre perfeccionables, rellenando los muros de contención de sensores, cámaras, pinchos y ganivetes de diferentes tipos.

De este modo se han perfeccionado los pasaportes, los más “modernos” (prácticamente todos) están proveídos de “micro chip” de etiqueta RFID... y toda el parafernalia de entrada, rayos X, detectores de metales, escáners, turnos de acceso son cada día más perfectos. Las visas de los países Schengen recopilan datos biométricos de los solicitantes (los 10 dedos de la mano y la cara... de momento), **los sistema de visados (VIS) conecta las embajadas y todos los puestos fronterizos de los países miembros.**

El poder (básicamente estados Y corporaciones) ha levantado los muros, pero de momento estos muros ni cubren todas las fronteras (habría que cerrar todas las playas...) ni son mínimamente eficaces.

Por eso se despliega toda una serie de aparatos tecnológicos, especialmente **vídeos con filtros espectrales o sin y cada vez más apoyados con software de reconocimiento automático** de acontecimientos sospechosos (videovigilancia inteligente http://negreverd.blogspot.com.es/2014/05/lull-de-lestat-una-mirada-cada-cop-mes_28.html).

En el estado español la vigilancia de la frontera recae sobre todo en la Guardia Civil (GC) y también en el Servicio de Vigilancia Aduanera (SVA), estos organismos disponen de un buen arsenal de vehículos aéreos, marinos y terrestres. Tienen el espaldarazo de sistemas de vigilancia aérea Y por satélite... y disponen de una amplia gama de sensores de todo tipo.

Entre enero de 2013 y agosto de 2014, la Guardia Civil ha invertido la suma del alrededores de 6,5 millones de euros. La mayor parte del presupuesto se ha destinado a cámaras térmicas (5,1 millones). Asensorizar las patrulleras de la Guardia Civil se han destinado 0,5 millones y a aparatos de visión nocturna 0,3.

El Servicio de Vigilancia aduanera, dependiendo de Hacienda, por el motivo que sea no ha tenido unos gastos tan grandes en gadgets tecnológicos (de hecho ellos se dedican sólo, básicamente, a temas de contrabando, dejando aparte el tema del flujo de personas), así que sólo han adquirido en el mismo periodo dos sistemas “optrónicos” de visión térmica y de visión diurna. Esto si, de los caros... un millón. Aparte de esto, a pesar de que nos consta que en sus embarcaciones y helicópteros disponen de cámaras térmicas, sólo han invertido en el mantenimiento de aparatos radiológicos de control fronterizo (para detectar a las desafortunadas “mulas”) por un importe de “sólo” 453.000 euros. Quizás los mantenimientos no superan los 18.000€ sin IVA del contrato menor o be se han empleado

sistemas de contratación por procedimiento negociado mucho más opacos.

Los contratistas adjudicatarios de los dos ministerios han coincidido con el adjudicatarios del Ministerio de Defensa (<http://negreverd.blogspot.com.es/2014/05/els-serveis-de-seguretat-de-lestat.html>).

En el caso del Ministerio del Interior (GC) el primero ha sido **la multinacional del armamento Thales** de rel francesa, con 930 mil euros es la séptima en volumen de contratación con el Ministerio de Defensa. La segunda ha sido Tecnobit, que se ha llevado 865 mil euros, es el sexto adjudicatario de defensa.

En el caso de Hacienda (SVA) lo principal ha sido la emprendida ex-estatal EADS Construcciones Aeronauticas S.A. que se ha llevado la contratación más importante por valor de un millón de euros.

El campo de los partidarios de la dominación también té sus mitologías, no todo son frías valoraciones técnicas y políticas.. **una de sus mitologías es el 100% de seguridad** (seguridad por ellos está claro), y esta seguridad esperan obtenerla aumentando el control tecnológico y así nos venden la prevención frente una invasión de pobres (los más pobres) que quieren consumir los recursos (escasos dicen) de los que disponemos.

De hecho muchas críticas (Cruz Roja, ACNUR...) se quejan de la brutalidad de los procedimientos de contención, básicamente de concertinas y balas de goma... si los métodos fueran más limpios (más tecnológicos) estas quejas quedarían neutralizadas y el muro no sería cuestionado.

Shenguen y las fronteras internas/ exteriorización: o sea las fronteras siempre más adentro y siempre más lejanas

Militarización y refuerzo estructural de la frontera como recurso para mejorar la circulación interna de shenguen.

De hecho el cierre de las fronteras, los largos controles, la dificultad de movimiento, por un lado pretende proteger el territorio nacional, por otro obstaculiza el libre movimiento de mercancía y turismo.

Alfano, el ministro de interior italiano, advirtió que el bloqueo del Brennero entre Italia y Austria –se temen interminables colas de turismo y camiones– acarrearía “enormes daños” económicos a los dos países, no sólo en el turismo sino en el transporte de mercancías y en la movilidad por razones laborales.

La situación actual en las fronteras entre Grecia y Macedonia o entre Italia y sus vecinas Francia y Austria, son un ejemplo de la dificultad que los estados europeos tienen para gestionar sus políticas defensivas por un lado y su necesidad de hacer circular el capital, por otro.

Actualmente en Grecia hay miles de personas atrapadas en la frontera, así como muchas hay en Ventimiglia. Con la llegada del verano los estado necesitan tener abierto el paso para dejar via libre al turismo, mientras que en Idomeni el estado griego tiene la necesidad de liberar la zona fronteriza para reactivar la circulación de trenes de mercancías.

La UE así prefiere no tener que gestionar directamente el problema de las personas migrantes y entregan (a cambios de miles de millones de euros) la responsabilidad de dicha gestión a estados externos.

La externalización de las fronteras se vuelve en una manera de no encarar el problema humanitario y de limpiarse las manos de los genocidios que se hacen en nombre la la protección de las fronteras. En la construcción del discurso sobre a necesidad de estas políticas migratorias agresivas, hay el tema de la peligrosidad migratoria, siempre con una mirada hacia el terrorismo como amenaza externa.

La amenaza migratoria justifica una parte muy grande de las operaciones militares que se efectúan en el mar mediterráneo.

El discurso del terrorismo que viene desde fuera, la migración irregular y la criminalidad transfronteriza, son las tres claves para justificar el hecho que Europa “militarmente tiene que defenderse”.

En todo este clima de paranoia anti-terrorista, construcción de vallas y muros y dificultad de gestión de

las puertas externas de Europa, como del flujo de capital entre los estados comunitarios, se está investigando sobre nuevas tecnologías que ayuden a gestionar los flujos.

La brutalidad TIC gira alrededor del uso de las TIC por el control de los accesos a los países, para evitar la entrada, en la práctica se disfraza de anti-terrorismo, de anti-mafia, pero este sueño sólo es una cortinas de humo...

Cómo en la mayoría de aplicaciones tecnodominadoras hay que ir a los EE.UU. para encontrar la fuente principal, aunque la UE tampoco se quedan demasiado atrás.

Después de los atentados del 11S los EE.UU. a través del Departamento de Seguridad Nacional (DHS) emprendió una serie de medidas para gestionar las entradas y salidas de sus fronteras ampliando lo **OS-VISITOR** (United States Visitor and Inmigrando Status Indicator Technology). Este sistema fue modificado y adaptado el 2013, bajo el nombre de **OBIM** (<http://www.dhs.gov/obim>), Oficina de Gestión Biométrica de la Identidad, también bajo el DHS.

El principal contratista del OBIM fue la multinacional de la consultoría Accenture. Accenture tiene su sede central en Irlanda y procede de la extinta Artur Andersen (la de la quiebra de EON), tiene aproximadamente unos 250.000 trabajadores y una sede en Barcelona, cerca de la zona universitaria de la Diagonal.

Accenture ganó un contrato del ministerio de trabajo español para poner en marcha un “plan de lucha contra la ocupación irregular y el fraude a la seguridad social”, por un importe de salida de 1,36 millones, con posibilidad de prórrogas y otras modificaciones contractuales. Un otro contrat bastante jugoso ganado por Acenture ha sido lo “concurso del siglo” (prácticamente 2.000 millones de euros) de la Generalitat de Cataluña, Accenture ganó uno de los lotes “aprovisionamiento y mantenimiento de aplicaciones” por un importe de 47,34 millones de euros... (fue el octau ganador, por detrás de Telefónica, T-Systems, Indra, IBM, HP, Fujitsu y ITTERIA)

Pues bien la OBIM tiene 30.000 usuarios autorizados de 52 agencias federales, oficinas de policía locales y gobiernos extranjeros (!?). El sistema crece constantemente, hace años podía procesar 75.000 consultas diarias... actualmente **OBIM identifica diariamente 5.000 visitantes, detiene unos 50 criminales en busca y más de 75.000 “presuntos”, realiza más de 13.000 identificaciones de huellas dactilares latentes, vigila además de 6 millones de personas de la “lista de terroristas” y procesa unas 400.000 coincidencias de identidad contra una base de datos de más de 160 millones de identidades individuales.** Cada comprobación de identidad a la frontera tarda 10 segundos al verificar la identidad de una persona y determinar si el viajero está a la “lista de terroristas”.

Los senado del EE.UU., recientemente ha aprobado un presupuesto por el 2015 la OBIM de 249 millones de dólares, 22 más que el 2014.

A la Unión Europea también disponemos de una buena base de datos, sobre todo desde la implantación del visado de Schengen (que incorpora la biometría facial y des 10 dedos de las manos) seguramente una buena parte de los 150 millones de individuos de la base de OBIM proceden de la de la UE.

Una buena parte del esfuerzo controlador de la UE se hace a través de la FRONTEX (<http://frontex.europa.eu/>), , http://www.iuisi.es/15_boletines/15_2009/formacion_guardia_civil_fronteras.pdf, www.cidob.org/es/content/download/6341/63571/file/16_gil_cast.pdf)

la agencia de gestión de fronteras exteriores, con sede en Varsovia. **Esta Agencia está en alza, su presupuesto desde su creación el 2005 hasta el 2013 a pasado de 6 a 90 millones de euros.**

FRONTEX está muy penetrada por los lobbys de las empresas de seguridad (INDRA, Thales, EADS, Selex, GMW...) que al mismo desarrollan y gestionan los softwares y las redes de comunicaciones de los sistemas de control, como los proyectos PERSEUS (INDRA y EADS....) 43 millones de euros,

SEABILLA (INDRA, Selex, Thales...)15 millones, TALOS (TTI Norte y la israelí IAI) 3.9 millones y OPEMAR (Thales, INDRA y Selex) por unos missers 669.000 euros.

FRONTEX, con un presupuesto de 244 millones parece ir tomando posiciones para ocupar el papel de controlador de fronteras exteriores que ahora tienen los estados, especialmente a través de EUROSUR (el proyecto de control de las fronteras del sur). De todas maneras la estructura presupuestaria de la UE, hace muy difícil averiguar si los recursos de FRONTEX son solamente estos 244 millones y que no dispone otros fondos, a través de lo Agencia Europea de Defensa, de fondos dedicados a la investigación y al estímulo económico o a la seguridad interior



El control de fronteras acontece evidentemente un gran negocio, se calcula que sólo el sector biométrico en el suyos usos militares y de control de fronteras generó el 2012 unos ingresos de 5.800 millones y se prevén ganancias de 15.800 millones por el 2021. En el momento en que la China y la India se incorporen totalmente a este mercado los beneficios pueden crecer exponencialmente.

El concepto de “**fronteras inteligente**” es la punta de diamante de estas investigaciones.

Una frontera vallada, militarizada, pero permeable a las mercancías y al turismo. Además muchas personas no comunitarias entran en el territorio europeo a través de regulares permisos de turismo, quedándose luego como ilegales.

Según una rueda de prensa de la Comunidad Europea : “Redunda en interés de la UE simplificar en la medida de lo posible el acceso a Europa de los turistas y viajeros de negocios, garantizando al mismo tiempo un nivel adecuado de seguridad.”

La iniciativa «Fronteras Inteligentes» consistiría en:

- **Un Sistema de Entrada/Salida (SES)** que registraría tanto el lugar y el momento de

entrada como la duración de las estancias breves autorizadas en una base electrónica de datos, en sustitución del actual sistema de sellado de pasaportes. A continuación esos datos se podrían a disposición de las autoridades de inmigración y control fronterizo.

- **Un Programa de Viajeros Registrados (PVR)** que permitiría, a determinados grupos de personas que viajan con frecuencia (por ejemplo, viajeros de negocios, miembros de familia, etc.) de terceros países entrar en la UE, sujetos a un examen previo apropiado, usando controles fronterizos simplificados en barreras automáticas. Así se agilizaría el cruce de fronteras de entre 4 y 5 millones de viajeros al año² y se fomentarían las inversiones en sistemas modernos y automatizados de control fronterizo (basados, por ejemplo, en pasaportes electrónicos) en los principales pasos fronterizos.

El control de los papeles ya no era suficiente, en la Europa iperracista las fronteras están por todos lados, exteriorizadas y también al interior, escondidas en un chip que registra datos biométricos de la persona migrante, las razones de porque ha entrado, la fecha de entrada y la en que tiene que abandonar el territorio.

Los harragas, los que queman los papeles para no poder ser identificados y expulsados, ya serán parte de una base de datos compartida entre todas las policías europeas, frontex y demás opresores. Portugal será el primer Estado miembro de la Unión Europea que ha puesto en prueba un nuevo programa de "fronteras inteligentes" diseñado para mantener controles más detallados en las fronteras exteriores durante las llegadas y salidas de los ciudadanos no comunitarios. **El plan será extendido en período de prueba a otros cinco países de la UE, entre los que se encuentra España.** Según las autoridades comunitarias, es crucial para identificar posibles amenazas terroristas.

El Sistema de Entrada/Salida está dirigido a hacer posible la grabación de la hora y el lugar de llegada y salida de los ciudadanos no comunitarios en los aeropuertos de la UE, mientras se aprueba el programa de registro del pasajero y sea posible para los visitantes frecuentes viajar bajo un sistema simplificado.

El programa va a ser probado durante seis meses en seis países de la UE, comenzando por Portugal que lo puso en marcha este fin de semana en el Aeropuerto de Lisboa. **Los otros cinco países donde será probado el sistema serán España, Alemania, Francia, Suecia y Países Bajos.**

El sistema ya había sido desarrollado antes de los recientes ataques en París, pero tras los sucesos, "la iniciativa ha ganado un nuevo impulso", ha afirmado.

El secretario de Estado de Interiores dijo que Portugal fue elegido, en parte, para ser pioneros en la aplicación del sistema debido a que en los últimos años el país ha desarrollado una serie de tecnologías de vanguardia en este campo.

Específicamente, el paquete de "fronteras inteligentes" fue propuesto por la Comisión en febrero de 2013. **El proyecto incluye la creación de un Sistema de Entrada/Salida y el programa de registro de viajeros (RTP).**

La CE destaca que "su objetivo es mejorar la gestión de las fronteras exteriores de los Estados miembros de Schengen, la lucha contra la inmigración irregular y proporcionar información sobre visado caducado, así como facilitar los cruces fronterizos para viajeros frecuentes previamente evaluados nacionales de terceros países".

Mientras tanto en el Estado español también se aplica esta tecnología a los puertos, en particular en la frontera Sur, la más vigilada por el estado. La Estación Marítima de Algeciras es la primera infraestructura portuaria en la que se ha desplegado el sistema de fronteras inteligente.

El Sistema de Paso Automatizado de Fronteras (ABC System), destinado a ciudadanos del Espacio Económico Europeo mayores de edad y que porten un pasaporte electrónico o un DNI electrónico, no solo agiliza los tiempos de paso en frontera, sino que conlleva además un incremento de la seguridad y facilita la interconexión con otros sistemas.

Comprobar la veracidad del documento de identificación electrónico, extraer la información referente a imagen y huella dactilar, capturar la imagen y la huella dactilar del pasajero en vivo y compararlas con las extraídas del documento de identificación electrónico, y controlar las bases de datos policiales para detectar a pasajeros con señalamientos en vigor, son los controles que realiza el sistema.

EL ABC System está operativo en los aeropuertos de Madrid, Barcelona, Girona, Palma de Mallorca, Alicante, Málaga y Tenerife Sur, y recientemente se ha implantado también en el paso terrestre entre La Línea de la Concepción y Gibraltar. La Estación Marítima de Algeciras es la primera infraestructura portuaria en la que se ha desplegado el sistema.

El Sistema de Paso Automatizado de Fronteras se enmarca dentro del Programa de Fronteras Inteligentes (Smart Borders), cofinanciado por la Comisión Europea, y cuyo objetivo es la integración de todas las fronteras aéreas, marítimas y terrestres.

El puerto de Algeciras está interesado por la **Operación Paso del Estrecho**. En el marco de una visita del ministro del Interior al Puerto de Algeciras, se ha presentado la "operación Minerva", cuyas principales misiones son el control de los flujos migratorios irregulares hacia la Unión Europea y combatir la delincuencia transfronteriza.

Este dispositivo, dirigido por la Policía Nacional y coordinado por Frontex, se activará el próximo 30 de julio, coincidiendo con la Operación Paso del Estrecho, y se desarrollará en los puertos de Algeciras, Ceuta y Tarifa. En el operativo participarán este año un total de 30 efectivos de la Policía Nacional y otros 48 agentes de 17 países de la Unión Europea.

En el estado español la creación y gestión de las fronteras inteligentes estará en las manos de la empresa Indra.

España da un paso más hacia adelante en lo que a **fronteras inteligentes** se refiere. El Ministerio de Interior, a través de la Secretaría de Estado de Seguridad, ha adjudicado a Indra el contrato para el desarrollo y la implantación del **Sistema de Registro de Nombres de Pasajeros (PNR)**, que entrará en servicio previsiblemente en mayo de 2016.

La implantación de esta nueva herramienta se enmarca dentro del despliegue en la Unión Europea de las fronteras inteligentes. Este sistema permitirá registrar los datos de pasajeros de **vuelos internacionales**, así como llevar a cabo un análisis de riesgos.

Asimismo, el Registro de Nombres de Pasajeros también permitirá explotar la información obtenida utilizando metodologías estadísticas, así como **realizar comprobaciones mediante búsquedas en fuentes policiales y fuentes abiertas en Internet, principalmente redes sociales.**

Desde la compañía explican que el sistema llevará cabo un análisis de toda la información disponible "para valorar cualquier posible riesgo y generar alertas relevantes para la lucha contra el terrorismo y el crimen organizado".

El PNR permitirá disponer de información con anterioridad al momento del cruce fronterizo. "Se lleva a cabo un análisis previo y exhaustivo de los riesgos del pasajero, empleando algoritmos complejos. Esto ayuda a las Fuerzas y Cuerpos de Seguridad a planificar las medidas adecuadas en caso necesario", asegura Indra.

Para llevar a cabo esta tarea, hará uso de tecnologías Big Data, un ámbito tecnológico en el que la multinacional mantiene "una fuerte posición de liderazgo internacional". Este conocimiento se suma a la experiencia de Indra en procesos de gestión de fronteras, tanto reguladas como no reguladas, y desarrollo de sistemas de inteligencia y seguridad.

La calidad técnica de la solución de registro de nombres de pasajeros ofertada permitió a Indra obtener en la licitación la máxima puntuación al aplicar los criterios fijados por el Ministerio de Interior para esta herramienta.

La multinacional se ha consolidado en pocos años como una de las empresas líderes en Europa en el desarrollo de sistemas de gestión de fronteras y soluciones para la movilidad, campo en el que participa activamente en **proyectos de I+D europeos, como ABC4EU (Automated Border Gates**

for Europe) o MobilePass, entre otros.

El pasado año, la compañía desplegó **sistemas biométricos ABC (Automatic Border Control), también conocidos como 'E-Gates'**, en los principales aeropuertos internacionales españoles (Madrid, Barcelona, Girona, Palma de Mallorca, Alicante, Tenerife Sur y Málaga) y en el puerto de Algeciras.

Estos sistemas verifican el pasaporte o DNI (en el caso de ciudadanos españoles) de los pasajeros de forma desatendida, contrastando sus datos con la información biométrica de su huella y rasgos faciales.

En total, Indra desplegó en España más de 100 'E-Gates' para agilizar el paso por frontera y evitar colas y molestias al viajero. Por el momento, su uso está limitado a ciudadanos del Espacio Económico Europeo mayores de edad que accedan al espacio fronterizo de la Unión Europea desde cualquier aeropuerto del mundo que no pertenezca a este Espacio.

Por otro lado, la compañía afirma que ha desplegado sistemas de vigilancia que protegen más de 5.000 kilómetros de fronteras en todo el mundo y remarca que es pionera en sistemas seguros de identificación, con más de 30 millones de documentos y cédulas de identidad expedidos en varios países. En el ámbito de soluciones de Inteligencia, Indra lleva años desarrollando "con éxito" soluciones tecnológicas.

Justo para dar un par de datos más sobre Indra: Sus sistemas proyectados a medida de los clientes (civiles o militares), dan respuesta a los requisitos operativos demandados sobre todo tipo de plataformas (tierra, mar y aire).

Cubren toda la gama de soluciones para el entrenamiento, desde los entrenadores más básicos, hasta los más complejos y completos sistemas de **simulación como los Full Flight Simulators Level Dy los Full Mission Defense Simulators.**

A nivel de defensa terrestre, **han instalado más de 5.700 km de fronteras** que son vigiladas por su tecnología. Además, han diseñado vehículos NRBQe para detectar e identificar amenazas nucleares, radiológicas, bacteriológicas y químicas.

En cuanto al mar se refiere, su tecnología responde en entornos adversos. Han desarrollado para los submarinos una antena combinada que permite hacer tareas de inteligencia de señales radar y de señales de comunicaciones de forma simultánea.

También compiten en el sector espacial (participan en el programa Galileo, la iniciativa espacial más ambiciosa impulsada por la Comisión Europea y la Agencia Espacial Europea) y en el ciberespacio, fundamental hoy día para los gobiernos. Asimismo, Francia utiliza sus sistemas de comunicación por satélite.

Además Indra y Thales han logrado un contrato del Ejército de 6 millones para los tanques.

Igualmente la tecnología de control fronterizo no deja nunca de actualizarse, es de septiembre 2016 la noticia que ha sido implantado un nuevo aparato de control de las fronteras españolas llamado CEFront. Apenas tiene ocho meses de vida, pero ya ha atendido miles de consultas y supervisado las 24 horas de cada día la actividad de los 80 puestos fronterizos de España. Es el **Centro Nacional de Coordinación de Puestos Fronterizos (Cefront)**, el "gran hermano" de la Policía.

Desde este centro, **ubicado en las instalaciones de la Comisaría General de Extranjería y Fronteras**, más de una treintena de agentes visualizan en tiempo real desde diferentes pantallas los puestos fronterizos -42 aéreos, 24 marítimos y 4 terrestres- para supervisar, coordinar y controlar todas sus actividades y reaccionar de manera inmediata ante cualquier incidencia.

El inspector jefe de la Policía Nacional Javier Núñez es el jefe de servicio del Cefront, impulsado por las instituciones europeas y el Ministerio del Interior y dividido en tres áreas: la de operaciones, la de estadística y la de análisis de riesgos.

Núñez explica a Efe que, además, el centro, enmarcado en el proyecto "fronteras inteligentes", es el punto de contacto en materia de fronteras tanto a nivel nacional como internacional.

Dentro del área operativa, el centro recibe todas las incidencias de los puestos fronterizos, las atiende y les da "respuesta operativa". También lo hace a todas aquellas entidades, como consulados, centros aduaneros o autoridades judiciales, entre otras, que requieren algún tipo de información.

En este sentido, Núñez indica que desde su puesta en marcha el centro ha gestionado los más de 7.000 correos electrónicos que ha recibido, a la vez que ha realizado 648 difusiones con información relevante a los responsables de las fronteras.

Todas las actividades que gestionan los puestos, como entradas y salida de territorio nacional, las solicitudes de asilo, los polizones y las actividades ilícitas que se detecten son recogidos en el área estadística, que analiza unos datos que permiten identificar, por ejemplo, el origen de las personas que entran, su destino, sus edades o su nacionalidad.

Y con todos esos datos estadísticos y los modus operandi que se detectan en los diferentes puntos, el Cefront realiza un análisis de riesgos para advertir a los puestos de las nuevas modalidades delictivas, como por ejemplo, las técnicas empleadas por las organizaciones criminales para falsificar documentos o las triquiñuelas utilizadas para poder entrar de forma irregular en el territorio.

Un informe que el Cefront remite también a otras unidades policiales que puedan estar afectadas.

Núñez resalta que todas las incidencias se recogen en un boletín mensual, donde quedan registrados todos los datos facilitados por los puestos.

El Cefront está en permanente contacto con la agencia europea Frontex y con otros centros nacionales como el de Aena o el de Salvamento Marítimo.

Porque lo importante, subraya el inspector jefe, es poder dar "una respuesta rápida y coordinada cuando exista cualquier incidencia".

Aunque el centro no gestiona la entrada de pateras con inmigrantes irregulares porque tienen lugar fuera de los pasos habilitados, sí lleva a cabo la estadística y el control de la evolución de este fenómeno en cooperación con otras agencias.

Otra de las amenazas que se persiguen desde este centro son las cada vez más sofisticadas falsificaciones de documentos, aunque la Policía también cuenta con nuevos sistemas técnicos capaces de detectarlas, concluye el inspector jefe.

Un apunte sobre la tecnología Big Data: La excusa, como pasa casi siempre, es la seguridad.

Ya no interesa el número de cámaras de control (aunque cada vez habrá más) sino otras cosas, el control automatizado sin operador humano, la detección de objetos, de situaciones, de actitudes y estados de ánimo, el reconocimiento de escenarios... Se trata de obtener sistemas que en tiempo real detecten objetos abandonados, identifiquen personas, identifiquen los objetos que traen, actitudes "sospechosas", sentimientos que permitan prevenir y prever situaciones de "riesgo" (brotes violentos, formación de concentraciones...).

Al mismo tiempo que se busca el análisis en tiempo real se busca también el acceso rápido en las enormes librerías de vídeo que generan los sistemas de vigilancia, los medios de comunicación y las redes sociales, la baja velocidad de acceso y la necesidad de mucha mano de obra humana (por visionado o para etiquetar escenas) han sido hasta ahora uno de los escollos más importantes por lo masivo de la información registrada en vídeo.

Poder hacer la investigación y seguimiento de un individuo a las grabaciones de las videocámaras de una calle comercial durante un largo periodo de tiempo o de escanear una red social buscándolo es una posibilidad demasiado tentadora porque cualquier controlador (poli, gobernando, estudios de los mercados...) pueda rehuirla.

En el informe “Big Data en los entornos de defensa y seguridad” editado por el Instituto Español de Estudios Estratégicos (IEEE) se marcan entre otros usos por las metodologías Big Data las siguientes ligadas con el videocontrol y las imágenes: Análisis de vídeo en tiempo real / investigación y recuperación rápida en librerías de vídeo e inteligencia visual en máquinas. De hecho ya hay al mercado programas con estas funcionalidades escaneados de archivos a 150fps (decenas a veces más rápido que el convencional) y localizaciones en bases de datos de 500.000 ítems en menos de un segundo.

El Estado Español, especialmente a través de su Ministerio de Defensa, pero también por medio de Universidades, gestores de infraestructuras y el sector privado participa en el desarrollo de estas herramientas.

Aparte de los ministerios de defensa uno de los sectores más interesados es lo de los transportes, especialmente ferroviario y aeropuertos y el control fronterizo.

BIOMETRIA, TECNOLOGIA Y AYUDA HUMANITARIA

YIDA, Sudán del Sur, 27 diciembre (ACNUR/UNHCR)- **La tecnología está cambiando todas las esferas de la vida, incluyendo las intervenciones humanitarias. En Sudán del Sur, ACNUR está usando imágenes de satélite, mapas interactivos, toma digital de huellas dactilares y envío de mensajes de texto para reforzar la protección de los refugiados, ayudar a los más vulnerables y llegar a los refugiados de las áreas urbanas.**

ACNUR está llevando a cabo el primer registro biométrico en Sudán del Sur usando tecnología digital de toma de huellas. **Los cerca de 200.000 refugiados han sido registrados en bases de datos estándar, pero la biometría ayudará a identificar a los refugiados más rápidamente**, de manera que puedan recibir una mejor asistencia.

En el campo de refugiados de Yida, el más grande de Sudán del Sur con más de 65.000 refugiados, la biometría es la manera decisiva para que ACNUR pueda orientar los servicios, evitar registros múltiples y hacer que la planificación y la prestación de servicios de asistencia sean más eficientes.

Al estar Yida muy cerca de la frontera, no es raro que los refugiados arriesguen sus vidas volviendo a casa para acompañar a otros miembros de la familia a un lugar seguro. Estos movimientos hacen que mantener unas cifras exactas de la población en Yida sea un desafío para ACNUR.

Un registro preciso también facilita el seguimiento individual de los refugiados más vulnerables, como Housna Ali Kuku, una madre soltera con cuatro niños que llegó a Yida a finales de julio. Una campaña de información en Yida le dijo a Housa cuándo debía llevar exactamente a sus niños al centro de registro de ACNUR.

“Me estoy recuperando de una infección en las vías respiratorias, y aunque estoy enferma y cansada, sé que es importante para mis hijos y vengo a ACNUR para que seamos registrados”, le dijo a ACNUR. Los niños de Housna no son conscientes de los esfuerzos de ACNUR por incorporar la alta tecnología a este proceso. **Uno a uno están siendo registrados y miran con fascinación a medida que el funcionario de registro hace rodar su dedo índice para capturar la huella digital de cada niño en el sensor de la pantalla de luz roja de la máquina.**

ACNUR está usando al mismo tiempo este procedimiento para actualizar información sobre situaciones de necesidades especiales, como mujeres cabeza de familia, mujeres embarazadas o en periodo de lactancia, o niños desnutridos. En este sentido, el personal de protección puede identificarlos rápidamente y satisfacer las necesidades de los más vulnerables en un campo formado en más del 70% por mujeres y niños.

El equipo también está registrando un nuevo dato: las direcciones de los refugiados. ACNUR ha estado trabajando recientemente con la ONG socia, ACTED, para tomar las coordenadas por GPS y poder hacer un mapa del asentamiento de Yida. Cada estructura o tienda está siendo incluida en el mapa.

Los mapas y las direcciones están vinculados a la base de datos de ACNUR, proporcionando valiosa información a través de la tecnología interactiva. Estos nuevos mapas permiten a los trabajadores humanitarios saber mucho más sobre la población del campo que mediante la mera localización de cada refugio, ya que la base de datos enlaza los datos geográficos y demográficos de cada familia.

“Ahora, detectar un problema está a un solo clic de distancia”, dice Emillie Poisson, Directora de ACTED para Sudán del Sur.

CAMPAMENTO DE THAM HIN, Tailandia, 30 de junio de 2015 (ACNUR) – La Agencia de las Naciones Unidas para los Refugiados ha completado la implantación de un sistema pionero que se utilizará para identificar a los refugiados de Myanmar acogidos en nueve campamentos sitios en la zona fronteriza de Tailandia.

Entre los meses de enero y mayo de este año, el ACNUR y el Gobierno Real de Tailandia verificaron y actualizaron, con la ayuda del nuevo sistema BIMS de gestión de identidad biométrica, los datos de casi 110.000 refugiados, registrados y no registrados, de Myanmar.

Se eligió Tailandia como país piloto para la implantación a nivel mundial de este sistema, que complementa los planes elaborados para verificar los datos biométricos de la población de los campamentos. Hace 10 años se suspendieron los registros habituales en los campamentos y la necesidad de disponer de información actualizada sobre la composición de las familias, los nacimientos, los fallecimientos y los matrimonios era cada vez más urgente.

Este ejercicio, llevado a cabo conjuntamente con los funcionarios del Ministerio de Interior, con el apoyo de ONG socias del ACNUR, exigió realizar un examen riguroso de los documentos disponibles y una verificación física de todos los núcleos familiares. Los líderes de los refugiados en cada uno de los campamentos ayudaron a movilizar a la población y la animaron a participar. El resultado es el examen más exhaustivo desde el punto de vista estadístico y de la protección realizado en 10 años de esta población de refugiados.

Gracias al sistema BIMS, por primera vez en la historia del ACNUR se obtuvieron las huellas dactilares y una imagen del iris de cada refugiado. Luego, estos datos se almacenaron de manera segura en la base de datos en línea del ACNUR y pueden consultarse desde cualquier lugar del mundo.

“En el futuro, la biometría será una ayuda para los refugiados, dado que el sistema garantiza que, una vez que estén registrados en el sistema y se hayan guardado sus huellas dactilares y sus iris, siempre sabremos dónde se encuentran”, dijo en Ginebra Sam Jefferies, Oficial Adjunto encargado de la implantación del sistema biométrico del ACNUR. “Si pierden la documentación, siempre pueden acudir a nosotros”.



© ACNUR/ R.Arnold

Una refugiada del campamento de Tham Hin examina su nueva tarjeta inteligente que contiene un enlace a los datos biométricos de su familia que figuran en la base de datos del ACNUR. Llevar el personal y la tecnología a algunas de las zonas más remotas de Tailandia planteó numerosos problemas logísticos. Fue necesario transportar dispositivos satelitales a campamentos que no disponían de línea telefónica ni acceso a Internet y cruzar ríos y recorrer durante 13 semanas cientos de kilómetros de serpenteantes carreteras de montaña a lo largo de la frontera entre Tailandia y Myanmar, cargando equipos delicados y transportando a más de 75 miembros del personal del ACNUR.

Al finalizar el ejercicio de verificación en Tailandia, se proporcionó a cada uno de los refugiados una tarjeta inteligente con datos biométricos y fotografías de su familia, que fueron cifrados de forma segura y pueden consultarse con los lectores de tarjetas del ACNUR incluso en lugares remotos sin acceso a Internet.

"Con estas tarjetas no necesitamos desplazarnos con equipos pesados, como por ejemplo, un servidor", dice Mireille Girard, Representante del ACNUR. "En los casos de regreso voluntario, nuestros equipos en Myanmar llevarán un lector de tarjetas en su mochila cuando realicen visitas sobre el terreno para documentar lo que ha ocurrido con los repatriados y verificar si han recibido asistencia para la reintegración. También transmitiremos esa información a otros agentes humanitarios y a las autoridades sobre el terreno para que puedan planificar y prestar servicios en los lugares en los que se necesiten".

"Esta verificación es muy importante para mí y para los demás refugiados. La tarjeta puede resultar decisiva para nuestra vida en el futuro. Si tenemos alguna posibilidad de regresar [a Myanmar], la tarjeta será una prueba válida ante el ACNUR o el Gobierno de Tailandia. Les digo a los otros refugiados que guarden su tarjeta inteligente en un lugar seguro, con sus pertenencias más valiosas", explica John Smith, un refugiado que trabaja para el Comité de Refugiados Karen en el campamento de Tham Hin, sito en la provincia de Ratchaburi.

QUE SON LOS DATOS BIOMETRICOS

La biometría, un término que proviene del griego *bio* (vida) y *metron* (medida), se dedica a desarrollar técnicas que permitan medir y analizar **una serie de parámetros físicos que son únicos en cada persona para poder comprobar su identidad.**

Entre los más utilizados están **la huella dactilar o el iris del ojo**, aunque los científicos también son capaces de identificar a un individuo **por su voz, su forma de caminar, su palma de la mano o los rasgos del rostro**.

Su tratamiento legal en España viene regulado por la Ley Orgánica de Protección de Datos (LOPD) de 1999 ([PDF](#)). Según recuerda un informe de la Agencia Española de Protección de Datos (AEPD) de 2006, la ley define en su artículo 3 los datos de carácter personal como **"cualquier información concerniente a personas físicas identificadas o identificables"**.

En el momento en el que dichos datos sí permiten la identificación de un individuo "resulta evidente que, en caso de procederse a su tratamiento dicho tratamiento deberá ajustarse a la LOPD", afirma la agencia.

El DNle español contiene datos biométricos, concretamente información sobre las huellas digitales, contenidas en el 'chip' de la propia tarjeta" Según informa el [Ministerio del Interior](#), el DNle español "permite realizar una identificación biométrica del titular de ésta, si bien esta función sólo estará disponible en puntos de acceso controlados".

Usos de los datos biométricos

Los datos biométricos se utilizan actualmente en los campos de **la seguridad, la medicina y del ocio**. Se usan para permitir el acceso a edificios o a zonas muy restringidas sin necesidad de utilizar tarjetas o claves de acceso que pueden transferirse fácilmente de una persona a otra.

La doctora española **Celia Sánchez-Ramos**, por ejemplo, ideó un sistema de identificación de personas a través de la **córnea** que le valió el premio principal del Salón Internacional de Inventiones de Ginebra de 2010, considerado el Nobel de los inventos.

Según explicó Sánchez-Ramos a EL MUNDO, no es posible replicar la cara interna de la córnea. **Incluso si el individuo se sometiera a cirugía ocular, el sistema seguiría identificándolo**. Por ello, este tipo de sistemas biométricos podrían usarse para iniciar la sesión en un ordenador, sacar dinero del cajero o utilizar el teléfono móvil sin introducir una contraseña con la certeza de que no se suplantarán nuestra identidad.

Bibliografía e link fronteras inteligentes y tecnología del control

- <http://ilmanifesto.info/come-leuropa-proteggera-i-confini/>
- <http://www.autistici.org/macerie/?p=32035>
- <http://www.autistici.org/macerie/?p=32031>
- http://www.hosteltur.com/110223_fronteras-inteligentes-aeropuertos-espana-participa-plan-piloto.html
- http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/4305484
- <http://www.onemagazine.es/nacional-defensa-indra-control-pasajeros-fronteras-inteligentes>
- <http://www.fmreview.org/es/tecnologia/hunt-orsak.html>
- <http://www.elandroidelibre.com/noticias/google-reconnect-tecnologia-para-ayudar-a-refugiados-en-alemania>
- http://protestantedigital.com/sociedad/39103/%E2%80%9CCLoveEurope_app%E2%80%9D_Ayudando_a_los_refugiados_a_encontrar_aquello_que_mas_necesitanhttp://protestantedigital.com/sociedad/39103/%E2%80%9CCLoveEurope_app%E2%80%9D_Ayudando_a_los_refugiados_a_encontrar_aquello_que_mas_necesitan
- <http://www.acnur.org/t3/noticias/noticia/un-sistema-biometrico-del-acnur-verifica-la-identidad-de-los-refugiados-en-tailandia/>
- http://noticias.lainformacion.com/politica/refugiados/sistema-basado-en-la-biometria-permite-a-refugiados-sirios-cobrar-subsidios-en-jordania_BjmZB0CMEHmknuxl80laQ3/

- <https://sites.google.com/site/controldecambioce/tecnologia-y-sociedad>
- <http://www.acnur.es/noticias/notas-de-prensa/1122-las-nuevas-tecnologias-ayudan-a-satisfacer-las-necesidades-de-los-refugiados-en-sudan-del-sur>
- http://europa.eu/rapid/press-release_IP-11-1234_es.htm
- http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/031_LAS_NUEVAS_TECNOLOGIAS_EN_LA_SEGURIDAD_TRANSFRONTERIZA.pdf
- <http://radioblackout.org/2016/05/niscemi-verso-unestate-di-lotta/>
- <http://www.lavanguardia.com/internacional/20160429/401439964485/italia-y-austria-tension-contenida-en-sus-fronteras.html>
- <http://negreverd.blogspot.com.es/2014/11/brutalitat-tic-tecnologies-de-la.html#more>
- http://www.iuisi.es/15_boletines/15_2009/formacion_guardia_civil_fronteras.pdf
- <http://negreverd.blogspot.com.es/2014/09/fronteres-civilitzacio-i-tecno-murs.html>
- http://negreverd.blogspot.com.es/2014/05/lull-de-lestat-una-mirada-cada-cop-mes_28.html#more
- <https://www.dhs.gov/obim>
- <http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Paginas/Inicio.aspx>
- <http://www.elmundo.es/espana/2013/12/05/52a0749d63fd3d8c498b456b.html>

Autor: persones del col·lectiu Te Kedas Donde Kieras (disolt).

SMARTPHONES Y REDES SOCIALES, UN ENFOQUE CRÍTICO.

Escribo de parte de un grupo (el col·lectiu contra el domini tecnològic “les hienes”) que tuvo una vida efímera. Empezamos juntándonos miembros de una misma asamblea universitaria para tratar el vasto tema de la tecnología. Veíamos a todo el mundo (también a nuestros compañeros) enganchados al teléfono móvil o a Internet. Compartíamos un rechazo y cierto desazón en la experiencia cotidiana de hablar con alguien y que éste estuviera constantemente mirando la pantalla de su *smartphone*. Al principio, constatamos como el tema nos afectaba profundamente y bromeamos sobre llamarnos Plataforma de Afectados por la Tecnología, parodiando a la PAH.

Viendo que la cuestión de la tecnología era tan grande, decidimos acercarnos a ella por esa parte que más nos tocaba diariamente: la sociabilidad. Nuestras formas de relacionarnos están cambiando muy deprisa. Hemos sido testigos en muy pocos años de una rápida penetración de los *smartphones* e Internet en la vida social. Nosotros creemos que los movimientos sociales anticapitalistas deberían haberse tomado un tiempo de reflexión antes de asimilarlos ciegamente, intentando comprender que dinámicas colectivas generan. No pretendemos negar su poder de difusión ni su realidad para así marginarnos aún más, tan solo queremos suscitar un debate que ha brillado por su ausencia.

Antes que nada, para analizar estas transformaciones, me gustaría que el texto partiera de una breve anotación sobre la propia materialidad de los *smartphones*. Muy a menudo, las discusiones sobre si la red es libre (y democrática) pasan por alto la naturaleza física de estos dispositivos en un afán de presentar Internet y toda tecnología como neutral y carente de ideología. Pero la realidad es otra, y en este caso sangrienta y brutal. Los condensadores de los teléfonos móviles están hechos de coltán, un mineral escaso en el planeta por el cual se libran guerras desde 1998. Solo entre 1998 y 2003 se contabilizaron unos 7 millones de muertos.ⁱ Además, la propia extracción del coltán genera también millares de muertos y enfermos puesto que los trabajadores se ven expuestos a la radioactividad de otros minerales que se encuentran bajo tierra junto al coltán. Detrás de estos conflictos bélicos está el financiamiento del FMI y de diversas empresas fantasmas de las cuales se benefician los productores de móviles.ⁱⁱ

Esta materia prima es transportada a fábricas chinas del sudeste asiático como la gigante Foxconn, que ensambla aparatos para Apple, entre otras marcas. Esta compañía, en la cual trabajan 1,2 millones de personas, es conocida por su trato inhumano hacia sus trabajadores: jornadas laborales de más de 10 horas, 6 días a la semana, horas extra impagadas, salarios de miseria... Bajo estas condiciones, en la planta industrial de Foxconn se han suicidado decenas de personas. A raíz de esto, la empresa decidió colocar unas redes para los trabajadores que se tiraban por la ventana, así como establecer un contrato laboral por el cual los empleados se comprometían a no suicidarse.

Hace dos años, uno de estos trabajadores decidió terminar con su vida. Era Xu Lizhi, un joven obrero de 24 años. Su caso apareció en algunos medios debido a su juventud y a que, en su escaso tiempo libre, se dedicaba a escribir poesía. Cito aquí parte de un poema suyo:

*Taller, línea de ensamblaje, máquina, tarjeta de fichar, horas extra, salario...
Ellos me han entrenado para volverme dócil
No sé gritar o rebelarme
Cómo quejarme o denunciar
Solo cómo sufrir silenciosamente el agotamiento.*

(...)

*Renuncio a faltar, renuncio a enfermar, renuncio a las faltas por asuntos personales.
Renuncio a llegar tarde, renuncio a irme temprano.
Por la línea de ensamblaje me mantengo firme como el hierro y mis manos vuelan.*

*¿Cuántos días, cuántas noches
habré estado - así - dormido de pie?ⁱⁱⁱ*

Y de la fábrica a la tienda nos encontramos en los escaparates esos móviles brillantes y relucientes en sus cajas de colores, completamente desconectados de las consecuencias sociales de su proceso de producción. Ni más ni menos que como cualquier otra mercadería que nos vendan.

Curiosamente, este ciclo de vida del teléfono termina, otra vez, en el continente africano. Ahí van a parar todos esos móviles estropeados o desechados.^{iv} En este sentido hay que hacer hincapié en su deliberada producción defectuosa para que tengan una fecha de caducidad. Se trata de la obsolescencia programada, aunque también hay que considerar la obsolescencia social, es decir, el hecho de que un móvil se considere pasado de moda y se cambie por otro con mejores prestaciones. En este punto hay que señalar la incesante presión que ejerce la publicidad para que compremos algo y, al cabo de poco, renovemos el producto.

Otro aspecto del que hablábamos en las charlas son las consecuencias ecológicas de la telefonía e Internet. Por ejemplo, hay enormes cifras sobre el gasto energético de las antenas repetidoras, los cables kilométricos que cruzan los océanos o la refrigeración de los centros de procesamiento de datos. También hay abundante documentación sobre los efectos que provocan en la salud las ondas del móvil y las redes wifi. Son otras formas interesantes de abordar la nocividad de Internet y los *smartphones* pero no las trataré en este texto puesto que, como he dicho, ya hay suficiente información al respecto.^v

El tema que realmente generaba debate en las charlas que hicimos con el colectivo era la parte referida a las consecuencias sociales del uso de Internet y los *smartphones*. También era el apartado que considerábamos más atractivo porque era el que notábamos más presente y nos hacía reflexionar sobre nuestra cotidianidad.

He aquí el quid de la cuestión. ¿Cómo nos afecta ese cambio de paradigma relacional?

Primero de todo, para decir simple y llanamente nuestra tesis, nosotras pensamos que el *smartphone* aísla y aliena al individuo, a la vez que fomenta el individualismo. Con esto no queremos decir que el ser humano fuese autónomo antes de la llegada de éste, más bien queremos señalar que el *smartphone* refuerza notablemente la estrategia capitalista de separar las personas y romper las comunidades humanas, o lo que quede de ellas.

Analizamos primero el *smartphone* como pantalla y, para entender que sucedía entre esta y nosotros, miramos hacia atrás para poder contextualizar mejor de dónde provenía. De esta forma, inscribimos al *smartphone* en una evolución histórica de la pantalla que, muy a grosso modo, la resumimos así:

El primer espectáculo de masas de la era industrial fue el cine. El cine es, tradicionalmente, un espectáculo colectivo, es decir, vemos la pantalla acompañados de más gente que, a menudo, no conocemos. Luego, entre los 60 y los 70 aproximadamente, en distintos países europeos se instauró la televisión en casi cada hogar. La pantalla entró en un ámbito doméstico y familiar, es decir, con menos gente y de confianza. Después, con los ordenadores e Internet, el consumo se volvió plenamente individual y desde casa, pero ya no desde el salón. Y así hasta llegar al *Smartphone* o teléfono inteligente, donde la pantalla se libera de sus ataduras para que la llevemos siempre encima.

Ver en perspectiva este periplo de la pantalla nos da algunas ideas. Hoy en día, fruto y continuación de ese transcurso histórico, las pantallas se multiplican a nuestro alrededor sumergiéndonos de lleno en la realidad virtual. Llevando un miniordenador en el bolsillo, esta segunda realidad es cada vez más inmersiva. La meta final de este proceso podría terminar en las Google Glass o en las gafas de realidad aumentada, ya promocionadas en la última edición del Mobile World Congress. En este sentido, también cabría destacar el furor generado por la aplicación Pokemon Go, de la que hablaremos más adelante.

Se podría haber ido aún más atrás para hablar de la relación filosófica entre el ser humano y la imagen, e incluso encontraríamos aportaciones interesantes en la caverna platónica o en la querella iconoclasta de los siglos VIII y IX, pero decidimos acotar un poco más el terreno. A quién sí utilizamos para nuestra crítica fue a Debord (*La sociedad del espectáculo*, 1967) para referirnos a la pantalla como eso que nos pone siempre en una condición de espectador, el cual es siempre un sujeto pasivo: la imagen aparece ante nosotros sin capacidad de poderla contestar, revelando así su carácter autoritario y unidireccional. En esta línea, el autor francés nos dice: *“El espectáculo se presenta como una enorme positividad indiscutible e inaccesible. No dice más que lo que aparece es bueno, lo que es bueno aparece”. La actitud que exige por principio es esta aceptación pasiva que ya ha obtenido de hecho por su forma de aparecer sin réplica, por su monopolio de la apariencia.*^{vii}

Esta inmersión en lo visual, este retraimiento en uno mismo que permite la pantalla portátil del *smartphone* es la que desconecta al individuo y lo fija temporalmente en otra realidad. Cuando decíamos que el *smartphone* aísla al individuo, a menudo pensábamos en ese silencioso vagón de metro en el que todas las personas van mirando su móvil, en un estado de semi-ausencia, separadas de su entorno físico.

Para entender la función del móvil en nuestra sociedad hundimos las raíces en las pulsiones más elementales del individuo. Todo ser humano tiene unas necesidades básicas: de comida, de casa, afectivas... En los ambientes que vivimos, especialmente en esas ciudades cada vez menos habitables, impersonales y con un creciente número de espacios privatizados, observamos que el móvil viene a suplir una carencia social de afectos y de comunicación. Un déficit que se hace más manifiesto en estas grandes urbes donde pasamos largas horas en esos no-lugares que son los transportes públicos^{viii}. Hoy en día, con la crisis se ha ido acentuando una tendencia hacia la precarización donde ya nada es estable: un día trabajamos aquí y otro allí, nos hemos mudado del barrio en que crecimos, los amigos de siempre también y nos vamos dispersando todos... a falta de espacio público o de comunidad por culpa de esa movilidad constante a la que estamos sometidas, el móvil se hace necesario para reconectar todas esas partes fragmentadas de la vida, para no quedarse demasiado solo y ser un infeliz. Los anuncios se adaptan a todo ese ambiente y te dicen “la vida es móvil”, “consúltalo estés donde estés”, “cuéntaselo a todos tus amigos”, “*connecting people*”... la publicidad, auténtico combustible del capitalismo, juega con nuestros sentimientos diciéndonos “Nunca estarás sola”, y claro, en este mundo monótono y asfixiante, ¿quién podría seguir viviendo sin la compañía o el afecto de las otras? Este sistema propone parches para los problemas que él mismo crea. Si este mundo rendido a la competición, la prisa y el trabajo ha sacrificado las relaciones humanas por el camino, es este mismo mundo el que te ofrecerá el móvil o Internet como remedio a esa enfermedad que ha generado.^{viii} Pero esa solución no es perfecta, pues no cura el dolor de la distancia, ni mejora las relaciones entre las personas, únicamente las hace pasar por otro canal.

La comunicación crea un indicio de comunidad. Entre la televisión y el *smartphone* hemos pasado (y estamos) por una época que, con sus más y sus menos, carece de conciencia de clase o de religión, de esos grandes relatos que aunaban la comunidad^x. Compartir fotos, chatear constantemente con amigos y, en general, participar del mundo online hace sentir al individuo formar parte de un todo. La simulación tecnológica provoca artificialmente una sensación de congregación.^x Parece cumplir con las características de ese espacio público cada vez más muerto que deviene en espacio virtual. Sin embargo, nosotros vemos la “comunidad virtual” como un oxímoron, ya que esta comunidad no junta a las personas para cantar al unísono, si no que, por lo contrario, Internet tan solo incita a publicitar nuestro aislamiento, creyendo que de la suma de aislamientos surgirá la comunidad.^{xi} La red solo une electrónicamente a los individuos, puesto que realmente cada uno de ellos está solo, en su cuarto o concentrado en su *smartphone*, separado del mundo. Volviendo a Debord: *“El espectáculo no es más que el lenguaje común de esta separación. Lo que liga a los espectadores no es sino un vínculo irreversible con el mismo centro que sostiene su separación. El espectáculo reúne lo separado, pero lo reúne en tanto que separado.”*^{xii}

Constatamos con el grupo que esta comunicación constante que facilitan las nuevas tecnologías muchas veces se vuelve en coacción. Pensamos que controlamos el móvil pero a menudo es él el que nos controla a nosotros, ya que cuando suena tenemos la obligación de mirarlo. En este sentido es sabido del alto número de parejas que han finalizado sus relaciones por el tema del doble *tick* del WhatsApp (¡Has visto el mensaje y no me has contestado!). Un estudio de 2013 afirmaba que 28 millones de parejas de todo el mundo habían terminado sus relaciones por culpa de esta aplicación^{xiii}. Asimismo, en lo que atañe al móvil en relación al mundo laboral tendríamos al dispositivo jugando aquí también el rol de controlador: el jefe te puede vigilar más y mejor. En muchos casos, la instauración del móvil ha significado para el trabajador el hecho de llevarse el trabajo a casa y así extender la jornada laboral más allá del horario marcado sin que la parte restante sea remunerada. En cuanto al control en el trabajo, ya han habido diversas sentencias judiciales sobre despidos improcedentes en pleitos sobre vigilancia de redes sociales de los superiores a los trabajadores^{xiv}. También tenemos otras expresiones del mismo asunto en fenómenos como el *cyberbullying* o el ciberacoso, los cuales están en el orden del día. En definitiva, lo que vemos en común en todos estos casos es que Internet no libera al individuo, sino que lo ata aún más a lo mismo que ya estaba atado antes: al trabajo, al jefe controlador, al novio machito que vigila, al matón del patio... La dominación se hace extensible más allá de las barreras físicas y de la presencia. Se perfecciona incluso.

Otro ejemplo que salió en uno de los debates, este quizá más trivial pero que sin embargo nos pareció ilustrativo, es la anticuada concepción de que no se debía llamar por teléfono a la hora de comer. Antes era de mala educación, ahora, en cambio, no contestar es quedar mal. De alguna forma, tanto en la vida laboral como en el resto de la vida, se nos dice que siempre tenemos que estar conectados, permanentemente en alerta.

Cada día que pasa se detectan más cambios en los comportamientos y las actitudes de las personas. Hechos que pueden parecer banalidades o nostalgias de cariz costumbrista, para nosotros indican el camino que tomamos de ahora para el futuro. Fijémonos también en la diana predilecta de toda publicidad, la juventud. En estos días que corren, para los adolescentes es un imperativo estar en las redes sociales (Facebook, Twitter, Whatsapp, Snapchat, Instagram...) y ser activo en ellas para no quedarse al margen de nada. La psicología afirma que en la pubertad y la adultez temprana es cuando se empieza a desarrollar la pertenencia al grupo y las redes, tal como he dicho, ofrecen una manera de amplificar la sensación de conexión con otras personas. En relación a esto, algunos investigadores han propuesto una nueva patología llamada FoMO (*fear of missing out*) que se puede traducir como “miedo a perderse algo”. Este fenómeno explica bastante bien la presión que siente algunos chavales por estar “dentro” del grupo, por no quedar marginados y ser objeto de burlas. Otra patología relacionada que nos puede resultar familiar es el denominado *ringxiety* (de *ring* y *anxiety*, ansia), en el cual sentimos vibrar el móvil y nos parece oírlo, cuando éste en realidad no está sonando.

¿Y por qué tanta adicción? ¿Por qué en todos lados gente mirando el móvil?

Cuando uno está en Internet, tanto desde el ordenador como desde el teléfono inteligente,

uno experimenta cierta sensación de confort y comodidad. Uno navega velozmente por la interfaz controlando cada detalle, mostrando lo que quiere mostrar, configurando hasta las más pequeñas cosas. El mundo digital aparece como un refugio del mundo real. Si la realidad para uno es desordenada, caótica, decepcionante y, en general, se tiene poca capacidad de decisión ella, el revés de la pantalla, la otra realidad, es gestionable, accesible, previsible y se le puede dar la forma que uno quiera. En un mundo masificado en el que unos estamos a merced de otros (o muchos lo estamos a merced de pocos) se nos permite ser minidioses en lo que atañe a nuestro mundo virtual, nuestro refugio-huida electrónica.

Lo que no controlamos son las consecuencias personales de cada uno en este giro colectivo hacia lo digital. La lógica del navegante de Internet es la dispersión y la multitarea. En la web se perciben constantemente estímulos de colores y formas que nos quieren llamar la atención para que pulsemos ahí. La gamificación pretende mostrar toda operación como un juego. De un sitio se va a otro y un clic alimenta otro clic, los ojos vuelan en diferentes direcciones. Por estas razones, Internet dificulta la capacidad de concentrarse en una sola cosa y, por lo tanto, tiende a sintetizar todo cada vez más, haciendo la lectura de más de 6 líneas algo inaceptable. Un ejemplo claro es Twitter.

Todo esto nos hace más dispersos e impacientes, necesitamos estímulos cada vez más inmediatos y todo es sujeto de cambio en cualquier momento. Lo sólido parece desvanecerse: cuando quedas con alguien, nunca sabes si el otro va a venir hasta que no lo confirma a última hora por Whatsapp. Se ha generado una nueva subjetividad. Y esta nueva subjetividad, como las anteriores, está condicionada por los instrumentos (los aparatos) que la burguesía (el capital) ha puesto sobre la mesa.

La circulación libre por Internet ha escondido la imposición obligatoria de su uso para relacionarnos. Si ya en los adultos y la gente mayor ha habido la necesidad de adaptarse y así generar nuevas dependencias, en los niños y los jóvenes hablamos de un crecimiento completamente condicionado por las redes sociales y los *smartphones* que van a empobrecer y degradar los conceptos de amistad o intimidad, reduciendo estos a la cantidad de mensajes y me gustas o al espectáculo que puede llegar a hacerse uno de su propia vida.

“Si al principio el móvil se asociaba al businessman, poco a poco se ha convertido en la herramienta imprescindible del ser humano liberal. Corresponde así a muchas de sus “cualidades” emblemáticas: individual, consumidor, moderno, flexible, eficiente, móvil, en comunicación permanente, etc. La difusión masiva y sin cuestionar del móvil ha participado de la propagación de estos valores, modificando en profundidad las relaciones sociales.”^{xv} En cuanto a objeto necesario y paradigmático de nuestra era, en cuanto mercadería que vincula las demás mercaderías, el *smartphone* se ha erigido como símbolo máximo de esta nueva etapa capitalista, así como lo fue anteriormente el automóvil.

r otro lado y cambiando un poco de tema, ¿cómo es toda esa comunicación telemática entre *smartphones* y ordenadores? Evidentemente un diálogo cara a cara es mucho más rico en particularidades que no una conversación de WhatsApp. Hay que considerar que aproximadamente un 80% de nuestra comunicación es no verbal. El filtro tecnológico elimina las diferencias para crear un lenguaje único y computable. En la red, las palabras se vuelven mensajes y las emociones quedan reducidas a emoticonos. De ahí esa ansia en llenar las frases con ellos y descubrir nuevos constantemente.^{xvi}

En este tipo de relaciones virtuales también tiene un gran protagonismo la imagen, sobre todo la de uno mismo. Hemos denominado este fenómeno como "cultura del postreo". Facebook, el ejemplo más claro, transmite una positividad absoluta: hay *me gusta*, pero no hay "no me gusta"; hay *amigos*, pero no hay "enemigos". La gente enseña lo maravillosa y alucinante que es su vida, como mercaderías autopromocionándose. Se muestran hipócritas, como si fuesen los actores de sus propias vidas. Es todo un universo virtual creciente que entendemos como una forma de evasión a una vida efectivamente miserable y aburrida.

*"La Jovencita es optimista, radiante, positiva, alegre, entusiasta,
en otros términos, sufre"*

"La Jovencita no se ama a sí misma, lo que "ama" es su imagen"^{xvii}

Además, gran parte de esta comunicación es espialable. Damos nuestros datos a "los amos de Internet" (Google, Apple, Facebook, Amazon) para que realicen estudios de mercado a partir de la perfilación de nuestras identidades digitales. Mediante el mecanismo perverso de la gratuidad aceptamos los TOS (*terms of service*, "términos de servicio") y facilitamos nuestra información a terceros, sin ser capaces de ver que si no hay producto que vender, el producto somos nosotros mismos. De nosotros sacan sus ingentes beneficios estas empresas que no venden nada físico.

En este sentido, el Big Data hace referencia a los grandes almacenes de información que, a partir del tratamiento de esos datos cedidos voluntariamente, permiten a las compañías conocer mejor a sus clientes, clasificar la población en grupos o segmentos dependiendo de diferentes variables (*clusters*) y, mejor aún, predecir las reacciones de los usuarios. El procesado de información que ejecuta el Big Data responde a una mezcla entre marketing y seguimiento policial, pero extendido al conjunto de la población. Cabe decir que sus intereses son mayoritariamente comerciales.^{xviii}

El Big Data es una fuente económica en plena expansión. Empresas como Google o Facebook, a pesar de no "producir" nada, atesoran unos ingresos altísimos que las equiparan a las más grandes multinacionales. La venta de datos personales es un sector relativamente nuevo, aparecido con la popularización de Internet. Hasta ese momento, la comunicación entre las personas no era una actividad de la cual se pudieran extraer tantos beneficios. ¿Qué quiero decir con todo esto?

El capitalismo aspira a monetizar (capitalizar) toda actividad humana. Su funcionamiento y la explicación de su expansión es la subsunción, es decir, absorber hacia el mercado aspectos previamente no capitalistas, subsumir actividades que no se rigen bajo la ley del valor, mercantilizar todas las facetas de la vida. El capital es valor valorizándose constantemente. Los parones y las caídas de ese proceso han producido crisis. Crisis que se han superado abriendo nuevos mercados, descubriendo nuevos sectores, dicho en otras palabras, poniendo el capital otra vez en movimiento. De la depresión del 29 se salió con la industria de la guerra arrasando con millones de vidas en la Segunda Guerra Mundial. De la crisis del petróleo del 73 se salió privatizando a ritmo neoliberal y convirtiendo el dinero en activos financieros para que pudiera seguir circulando pese a ser ficticio. Hoy en día, también en crisis (permanente), vemos un enorme campo a experimentar en el Big Data y la realidad virtual. Las ganancias de Facebook o Google así lo certifican. El fenómeno Pokémon Go también nos lo demuestra: la realidad aumentada crea una capa que encubre el espacio público para privatizarlo.^{xx} Este juego, del cual Google también participa, ha marcado récords de beneficios (Nintendo ha duplicado su valor en bolsa) además de dar lugar a situaciones dantescas como la de la niña estadounidense que fue atropellada por un coche mientras capturaba Pokémon y que luego criticó la aplicación, acusándola de ser la causante de su accidente.^{xx} En conclusión y ya finalizando,

para sintetizar este cambio de paradigma en las relaciones, me acojo a una reflexión que aparece en el último libro del comité invisible.

Esta catástrofe es en primer lugar existencial, afectiva, metafísica. (...) No ha sido a la ligera que [el hombre occidental] ha puesto tantas barreras entre él y el mundo. Arrojado sin tregua de la euforia al estupor y del estupor a la euforia, hace el intento de remediar su ausencia en el mundo con toda una acumulación de especializaciones, de prótesis, de relaciones, con todo un montón de chatarra tecnológica al fin y al cabo decepcionante. De manera cada vez más visible, él es ese existencialista superequipado que solo para cuando lo ha ingeniado todo, recreado todo, al no poder padecer una realidad que, por todas partes, lo supera. (...) La vida está efectivamente, afectivamente, ausente para él, pues la vida le repugna; en el fondo, le da náuseas. Es de todo aquello que lo real contiene de inestable, de irreductible, de palpable, de corporal, de pesado, de calor y de fatiga, de lo que ha logrado protegerse arrojándolo al plano ideal, visual, distante, digitalizado, sin fricción ni lágrimas, sin muerte ni olor, de Internet.

(...) No es el mundo el que está perdido, somos nosotros los que hemos perdido el mundo y lo perdemos incesantemente; no es él el que pronto se acabará, somos nosotros los que estamos acabados, amputados, atrincherados, somos nosotros los que rechazamos de manera alucinatoria el contacto vital con lo real. La crisis no es económica, ecológica o política, la crisis es antes que nada de la presencia.^{xxi}

No nos gusta la vida que vivimos (¿a quién le gusta verdaderamente?) y por lo tanto huimos de esa realidad a base de drogas, series y fiestas al fin y al cabo deprimentes. Interponemos entre nosotros y el mundo un *smartphone*, una pantalla, una *barrera*, que tape un poco. Sentimos que estamos solos y que todo da asco, pero entonces miramos al móvil y vemos que tenemos un mensaje y pensamos: "bueno, al menos alguien piensa en mí". Es una permanente huida hacia adelante, hacia el abismo.

Como alternativa, nosotros como grupo suplíamos esa comunicación vía móvil e Internet por encontramos diariamente en el local de estudiantes. Nuestra propuesta, un poco vaga y difusa, es recuperar los espacios públicos y colectivos: hacer vida en ellos, encontramos *afectivamente* en los ateneos, en las plazas, en el barrio, en las asambleas, en el sindicato... Que esto, en el fondo, no es más que la antigua historia de la clase obrera, la cual se juntaba en estos sitios para conspirar y compartir *emocionalmente* sus miserias. Se trata de recuperar la cultura local enfrente de la cultura capitalista o la cultura del espectáculo. Recuperar la historia de los barrios combativos, tratar de hacer habitables nuestras vidas, atacar aquello que las degrada y las mata.

Joan Liébana
(capitaludd@nodo50.org)

ⁱ Con esta cifra situamos el genocidio del Congo en el segundo puesto de las guerras con más víctimas fatales justo por detrás de la Segunda Guerra Mundial. Asimismo, bajo la escalofriante cifra de 7 millones, tampoco queríamos olvidar el alto número de mujeres violadas, torturas, migraciones forzadas, deforestación, mutilaciones o el uso de niños soldado.

El tema de la guerra en el Congo está suficientemente documentado y por lo tanto no será el principal interés del texto profundizar en este aspecto. Des de aquí recomendamos la lectura del capítulo "El ejemplo del coltán" dentro *Cuadernos de negación, nº8 Crítica a la razón capitalista* <<http://cuadernosdenegacion.blogspot.com.es/2013/12/nro8-critica-de-la-razon-capitalista.html>>, DE ALTUBE, RAMIRO (2004) *El imperialismo continúa, la fiebre del coltán*. <<http://www.rebelion.org/noticia.php?id=2727>>, y DE ALTUBE, RAMIRO (2011) *La fiebre del coltán, genocidio en la República Democrática del Congo*. <<http://www.rebelion.org/noticia.php?id=138707>>

ⁱⁱⁱ Recomiendo enardecidamente sus poemas. En esta web se puede encontrar algunos más <http://www.sinpermiso.info/textos/obituario-de-un-cacahuete-la-poesia-obrera-de-xulizhi-0>

^{iv} ¿Dónde van los móviles que ya no queremos? (2012) Expansión (diario) <<http://www.expansion.com/accesible/2012/10/11/empresas/1349987490.html>>

^v Este artículo da algunas cifras sobre esta cuestión *Vivimos rodeados de radiaciones electromagnéticas*, Moai: boletín sobre control tecnológico, biológico y social. <http://archivomoai.blogspot.com.es/2013/04/vivimos-rodeados-de-radiaciones_28.html>

^{vi} DEBORD, GUY (2002). *La sociedad del espectáculo*. Valencia, España, Pre-Textos.

^{vii} Considerábamos como otros no-lugares Internet (la red): el espacio virtual, ese espacio que no es espacio. Bajo esa idea de no-lugar también nos venía a la cabeza ese tipo de plazas hechas por urbanistas de nuevo cuño, en las cuáles predomina el diseño más que las necesidades humanas. Esas plazas que tienen el suelo duro, que parecen más hechas para el tránsito de las personas y los coches que no para el encuentro, que permiten una gran visibilidad para detectar rápidamente las conductas incívicas, que a menudo los bancos están dispuestos de formas extrañas en las que la gente no pueda hablar entre ella.

^{viii} Capítulo "Más aislado" dentro de *Quema tu móvil*, (fanzine) <https://quematumovil.pimienta.org/mas_aislado.html>

^{ix} Exceptuamos aquí la comunidad musulmana que sí mantiene en gran medida su religiosidad.

^x IPPOLITA (GRUPO). (2016). *Ídolos: ¿la Red es libre y democrática? ¡falso!* Madrid, Enclave de Libros.

^{xi} *La xarxa...* (poema) (2010) < <https://invisiblecomite.wordpress.com/2010/03/06/la-xarxa/>>

^{xii} DEBORD, GUY (2002). *La sociedad del espectáculo*. Valencia, España, Pre-Textos.

Xiii

La culpa no es del doble 'check': el verdadero papel de WhatsApp en las rupturas de pareja, (2015) El diario (diario)

<http://www.eldiario.es/hojaderouter/Internet/Whatsapp-relaciones-problemas_de_pareja-detectives-abogados-consejeros_matrimoniales_0_348915726.html>

^{xiv} VALERO MOLDES, FABIÁN. (2013), *La actividad en las redes sociales como causa de despido* <[http://www.elderecho.com/laboral/actividad-redes-sociales](http://www.elderecho.com/laboral/actividad-redes-sociales-causa-despido_11_570430002.html)

^{xvi} *Por fin la paella valenciana tendrá su emoji en WhatsApp*, (2016), 20 minutos (diario) <<http://www.20minutos.es/noticia/2749454/0/paella-emoji-icone-emoticono-whatsapp/>>

^{xvii} TIQQUN (GRUPO). (2012). *Primeros materiales para una teoría de la Jovencita ; seguido de "Hombres-máquina: modo de empleo"*. [Madrid], Acuarela.

^{xviii} El procesado de datos con fines mercadotécnicos es ampliamente superior al uso de estos datos para fines políticos, es decir, para la investigación y la vigilancia de los individuos. A propósito de esta vigilancia virtual, destaca el programa estadounidense PRISM, un dispositivo secreto de control masivo de [Internet](#) y de las telecomunicaciones que fue desarrollado por la Agencia Nacional de Seguridad ([NSA](#)). El impacto global del programa fue denunciado en junio de 2013 por el revelador Edward Snowden. Prism cuenta con la colaboración de Microsoft (comprendiendo también Skype), Google (y Youtube), Facebook, Yahoo!, Apple, AOL i Paltalk. Fue curioso como fue ferozmente reprochado el gobierno de Obama por esta iniciativa, pero en cambio apenas fueron criticadas estas corporaciones multinacionales que sin su contribución el programa PRISM no hubiera funcionado.

^{xix} El fenomen Pokémon, (2016) Solidaridad Obrera (diario) <<http://lasoli.cnt.cat/12/08/2016/el-fenomen-pokemon/>>

^{xx} Esta chica sufre un atropello cuando cazaba pokémon y dice que la culpa la tiene el juego, (2016) La Vanguardia
<<http://www.lavanguardia.com/tecnologia/videojuegos/20160715/403234086296/chica-sufre-accidente-de-coche-por-jugar-a-pokemon-go.html>>

^{xxi} COMITÉ INVISIBLE (FRANCIA). (2015). *A nuestros amigos*. Logroño, Pepitas de Calabaza.



