ALGUNOS EJEMPLOS DE ESPIONAJE Y VULNERACIÓN DE LA PROTECCIÓN DE DATOS A ESCALA MUNDIAL[1]

Examples of spionage and vulneration of data protection, on a world order

POR: DRª ROSA MARÍA RICOY CASAS
Profesora Contratada Doctora de Ciencia Política y de la Administración
Universidad de Vigo (España)
rricoy@uvigo.es; rricoy@uned.es

RESUMEN: La política ha de considerarse como una práctica, proceso o actividad orientada a la regulación del conflicto y a la consecución de objetivos colectivos, siendo su resultado la adopción de decisiones que obligan a los miembros de la comunidad. Las instancias supranacionales y mundiales asoman por la fuerza de los hechos en el horizonte político del planeta, propiciando nuevas formas y estructuras políticas e institucionales, nuevas formas e imágenes de gobernabilidad, más amplias, integradoras y globalizadas. Asimismo, se confirma la necesidad de esta tendencia de establecer una estrecha interconexión entre lo local, lo nacional y lo global, produciéndose al mismo tiempo un gradual desbordamiento y perforación del sistema de soberanía estatal. Ámbitos como la protección de datos o el espionaje a nivel internacional avalan esta tesis e imponen un cambio de paradigma jurídico y político para hacer frente a esta nueva realidad global.

PALABRAS CLAVE: Gobernanza global y Glocal, espionaje, protección de datos, derechos fundamentales, Estado de Derecho.

ABSTRACT: The policy (politics in general) must be considered as a practice, process or activity oriented to the regulation of the conflict and to the achievement of collective objectives, the result of which is the adoption of decisions that obligate the members of the community. The supranational and global instances (all over the world) emerge from the force of events in the political horizon of the planet, fostering new forms and political and institutional structures, new forms and images of governance, broader, integrating and globalized. It also confirms the need for this tendency to establish a close interconnection between the local, the national and the global, producing at the same time a gradual overflow and drilling of the system of state sovereignty. Areas such as data protection or espionage at the international level endorse this thesis and impose a change of legal and political paradigm to face this new global reality.

KEYWORDS: Global and Glocal Governance, espionage, data protection, fundamental rights, Rule of Law.

[1] * Recibido para publicación: 9 de enero de 2017.
Enviado para evaluación externa: 10 de enero de 2017.
Recibida evaluación externa positiva: 3 de octubre de 2017.
Aceptado para publicación: 20 de diciembre de 2017.

SUMARIO: I.- INTRODUCCIÓN. II.- ESPIONAJE Y PROTECCIÓN DE DATOS. III.- III.- LA CONSTATACIÓN DE LA CRISIS DEL ESTADO-NACIÓN PARA HACER FRENTE A LOS RETOS DE GOBERNABILIDAD DE LAS SOCIEDADES EN LA ERA GLOBAL. LA NECESIDAD DE UNA GOBERNANZA GLOBAL. IV.- ALGUNAS CONCLUSIONES. V.- BIBLIOGRAFÍA.

I.- INTRODUCCIÓN

La constatación de la crisis del Estado-nación para hacer frente a los retos de gobernabilidad de las sociedades en la era global, conduce inexorablemente al cuestionamiento de la propia teoría del Estado tradicional. El actual sistema internacional hereda los más destacados problemas y dinámicas de la Guerra Fría, agravados por algunos de los efectos negativos de la globalización (con mayor complejidad y dinamismo), haciéndose cada vez más difícil reconocer cuál es el campo específico de lo propiamente "internacional", modificándose los límites clásicos de los Estados. La expansión del terrorismo a nivel nacional e internacional, la consolidación de la sociedad del riesgo, la invasión de una cultura punitiva, o el fenómeno de *délocalisation* de internet, se perfilan como ejes imprescindibles en el análisis de las transformaciones del Estado y la realidad jurídica y política actual. A las antiguas teorías geopolíticas deben sumarse nuevas concepciones de la esfera política global. Tal vez al concepto de "Sociedad Post-Estatal", se una la idea del "desbordamiento de los espacios geoestatales", y añadir el cuestionamiento de ¿cuál es el Gobierno de la Globalización? Ello constituye, verdaderamente, una teoría politológica del Estado del siglo XXI. Asimismo, ejemplos de la teoría del "linkage" entre la política internacional y la nacional, el enorme desarrollo del *Espacio de Libertad, Seguridad* de la Unión Europea, las recombinaciones de alianzas o *partnership* entre los diversos Estados según las cambiantes situaciones, y otros ámbitos en los que se encuentran involucrados importantes conceptos como razón de Estado o Soberanía.

Así, mientras en el pasado se necesitaban importantes recursos materiales y humanos para ejercer influencia política o económica a escala global, las fronteras se han hecho permeables conforme el poder se traslada del mundo físico al mundo virtual. El uso malintencionado o incorrecto de innovaciones de las que se puede tener conocimiento por el acceso a la información a través de internet y el espionaje por parte de agentes criminales, otros estados o grandes multinacionales (industria armamentística o en campos de investigación tecnocientífica, como la biotecnología, la nanotecnología, la genética o la inteligencia artificial, entre otros) puede comprometer la seguridad internacional. Asimismo, el control de la información sobre los individuos y corporaciones, por la huella digital que dejamos (en ocasiones bajo el no veraz fin de garantizar la seguridad mundial), se convierte en una eficaz y potente herramienta por parte de gobiernos y corporaciones, que resulta muy peligrosa si se hace un uso pernicioso de la misma, conllevando una exposición y pérdida de libertades individuales, en muchos casos sin conocimiento, y en otros tantos intolerables. Se pretende mostrar esta realidad a través de numerosos ejemplos sobre la interceptación ilegal de comunicaciones por parte de Gobiernos y Corporaciones, las técnicas

utilizadas, y la reflexión sobre la necesidad de una gobernanza internacional en dicho ámbito que proporcione un espacio seguro, pero que también garantice de manera proporcionada, la protección de los derechos fundamentales de los ciudadanos y sin mero fin comercial.

II.- ESPIONAJE Y PROTECCIÓN DE DATOS

Primero fueron las cámaras de seguridad en bancos y cajeros, más tarde, cientos de cámaras en lugares públicos, y ahora una intromisión en qué y a quién escribimos o llamamos. Pronto todas las facetas de nuestra vida podrán ser controladas con la excusa de la seguridad. ¿Cuál es el límite? ¿Hasta dónde estamos dispuestos a ceder a cambio de la ilusión de seguridad (o al menos gran seguridad)? En la actualidad ya se han creado potentes sistemas estatales de seguridad, pero surge el nuevo dilema con los sistemas que no siempre responden a los cauces y exigencias de las sociedades democráticas, ya que, en la práctica, imponen a los ciudadanos la aceptación resignada de la intromisión en algunos de sus derechos más importantes. Echelon[2], Carnivore[3], Enfopol[4], o Sitel[5], son algunos ejemplos y la muestra palpable de los riesgos que para la

[2] *Echelon* es un sistema de interceptación de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda. Sus dos principales características, frente a otros sistemas de espionaje, son: su capacidad para ejercer un control simultáneo de todas las comunicaciones. Todo mensaje enviado por fax, teléfono, Internet o e-mail, con independencia de su remitente, puede captarse mediante estaciones de interceptación de comunicaciones, lo que permite conocer su contenido. Se trata de un sistema que funciona a escala mundial gracias a la colaboración e interacción de los Estados *supra* citados, lo cual posibilita una vigilancia a nivel mundial de las comunicaciones por satélite.

[3] *Carnivore* es un sistema de sofware y hardware con capacidad para localizar y perseguir las comunicaciones de un usuario de Internet. El sistema interviene la comunicación en un punto estratégico, como es el ISP (Proveedor de Servicio de Internet) -servidores que todos los internautas utilizamos para conectarnos a Internet-. Cada palabra que escribimos o ejecutamos siempre es recogida por el ISP que nos da acceso a la Red. La *Caja Negra* del FBI se instala en el servidor del ISP. Pero además de *software*, el FBI incluye el *hardware* compuesto por una PC ensamblado en una caja modelo Rack para que pueda incorporarse fácilmente en las redes del ISP, como si fuera un concentrador o un "router" más, sin necesidad de dispositivos externos.

[4] *Enfopol* del inglés "Enforcement Police" (policía de refuerzo), es un sistema de interceptación de las comunicaciones de la Unión Europea que surge como respuesta al megasistema ECHELON, propiedad de Estados Unidos, el Reino Unido y varios países miembros de la Commonwealth. intenta imponer sus normas a todos los operadores europeos de telefonía fija y móvil para que la policía secreta europea tenga acceso total a las comunicaciones de sus clientes, así como a la información sobre los números marcados y los números desde los que se llama. En el caso de Internet, "los proveedores deben facilitar "una puerta de atrás" para que puedan penetrar a sus anchas en los sistemas privados. Además, están obligados a informar sobre los datos personales de sus clientes (datos de correo electrónico y claves privadas). Todo sin que sea necesaria una orden judicial" (AÑOVER, 2001).

[5] *Sitel* (Sistema Integrado de Interceptación de Telecomunicaciones) es un avanzado sistema informático desarrollado por la multinacional Ericsson, que ha permitido la interceptación sin límite, de todas las telecomunicaciones que tuvieran lugar en España, y es utilizado conjuntamente por las Direcciones Generales de Policía y Guardia Civil, así como por el CNI (Centro Nacional de Inteligencia). Además de interceptar las comunicaciones, permitía recoger un paquete de datos conocido como "información asociada a la comunicación". Con el sofisticado software desarrollado, los Agentes podían pinchar directamente los teléfonos sin tener que contar con las operadoras telefónicas y podían tener acceso tanto a las conversaciones como a la identidad de los comunicantes, el lugar desde donde están hablando, el operador telefónico e incluso el contrato de servicio suscrito con ese operador. Y todo eso en tiempo real.

libertad de los ciudadanos implica la creación de sistemas de seguridad y control no sometidos a supervisión por parte de instancias internacionales garantes de que la persecución de criminalidad en la Red no pueda degenerar en una vigilancia incontrolada de millones de ciudadanos pertenecientes a todos los países del mundo.

En todo caso, si hoy se conocen algunas de estas prácticas, que ni siquiera se filtran y menos debaten a través de los resortes de los Parlamentos Nacionales (curiosamente tampoco en el debate público), es gracias –entre otros- al espionaje (entre países e industrial). Los intereses económicos de países y multinacionales han sido la causa que ha llevado este sistema al debate público: la interceptación de las comunicaciones entre Thomson-CSF y el Gobierno Brasileño para la negociación de un contrato millonario para un sistema de supervisión por satélite de la selva amazónica permitió la concesión del proyecto a la empresa estadounidense Raytheon, vinculada con la red Echelon (RODRÍGUEZ PÉREZ, 2008); la interceptación de los faxes y las llamadas telefónicas entre Airbus y el Gobierno de Arabia Saudí con los detalles de las comisiones ofrecidas a los funcionarios, permitió a Estados Unidos presionar para que el contrato de un billón de pesetas fuera concedido a Boeing-McDonnell Douglas en 1995; o la interceptación de las comunicaciones entre el Gobierno de Indonesia y representantes de la empresa japonesa NEC, en relación con un contrato de 200 millones de dólares en equipamiento de telecomunicaciones, permitió a George Bush intervenir personalmente para obligar a Indonesia a dividir el contrato entre la NEC y la firma estadounidense AT&T (PACHÓN OVALLE, 2004: 5).

Todos hemos conocido a través de los medios de comunicación, aunque lo suponíamos de la mayoría de países debido a que el espionaje entre territorios es una práctica ya realizada en la época romana, que la Agencia Nacional de Seguridad de Estados Unidos (NSA) espió las llamadas telefónicas de 35 líderes mundiales (informaciones filtradas por Edward Snowden, ex agente de este organismo, al diario británico "The Guardian"). Muchos de ellos supusieron, tras la revelación a los medios, un auténtico conflicto diplomático. Detrás de este tipo de actividades puede observarse el interés no sólo de recabar información, sino de mantener su liderazgo (aprovechando su liderazgo tecnológico); de expresar su hegemonía en este aspecto incluso con los que señala como homónimos en la concertación internacional y diplomática; de vigilar a las potencias emergentes para que no pongan en peligro el equilibrio de poder que lidera ni el dominio geopolítico sobre los "grandes espacios"; controlar a sus enemigos manifiestos (Rusia sigue siendo objetivo prioritario de sus operaciones de ciberespionaje); el control de las principales organizaciones internacionales, adversarios en la lucha global por el control del planeta; o poner en práctica acciones masivas dirigidas a ejercer un control de la conducta y del pensamiento de los usuarios de la Red Global.

Informes de los Ministerios de Justicia y de Defensa, y del Consejo General del Poder Judicial, denunciaban importantes problemas de cobertura legal. En junio de 2006, la Fiscalía de Madrid eleva un informe al Fiscal General del Estado, advirtiendo que SITEL estaba siendo utilizado sin cobertura jurídica adecuada y que el Reglamento de 2005 no tenía rango suficiente para dar garantías constitucionales, puesto que, conforme a la Constitución, este debería de ser regulado mediante Ley Orgánica. Asimismo, se producían otros problemas, porque se han estado utilizando certificaciones digitales que permiten identificar al responsable de la información, pero que o permitían certificar si lo que contenía el archivo era auténtico; no se almacenaban adecuadamente y se hacía sine die, etc **(**DÍAZ, 2009).

Posiblemente puede parecer utópico pensar que los gobiernos dejen de espiar a sus ciudadanos, ya que la mayoría de los programas que utilizan, no todos, aunque sin ser creados bajo el debate oportuno, están apoyados por coberturas legales, muchas de ellas de lo más peregrino, otras tantas cuestionables pero legales, y siempre en manos de decisiones políticas. Quizás tan poco realista como la aplicación práctica que tendrán ciertos acuerdos para limitar el espionaje internacional por la ONU, pese a su respaldo unánime por la comunidad internacional. Es suficientemente simbólico que Washington hubiera apoyado el texto tras lograr (con el apoyo de Reino Unido, Canadá, Australia y Nueva Zelanda), rebajar el tono de parte de la redacción.

Asimismo, hoy en día ya sabemos que los datos informáticos de bancos, gobiernos y grandes multinacionales es material preciado. También los políticos de regímenes autoritarios que quieren disponer de un lugar seguro para guardar información con la que negociar o incluso salvar la vida. La información más sensible e importante del mundo se esconde, entre otros lugares, en el búnker suizo "Swiss Fort Knox" en un túnel excavado por el Ejército suizo durante la Guerra Fría. Desde hace tres años custodia la cápsula del tiempo del proyecto Planets, en el que participaron 16 universidades europeas. Es un recipiente de metal sellado dentro del cual están las herramientas necesarias para descifrar todos los formatos de archivos que se conocen en la actualidad, algo así como la piedra de Rosetta de la era digital[6].

Los internautas buscan alternativas para proteger su intimidad: utilizar otro sistema operativo fuera de los tradicionales como Apple, Google Chrome y Microsoft Windows; cambiar de navegador, buscador, redes sociales, sistemas de mensajería y correo electrónico, etc masivos, y utilizar otros más seguros. Quizás refuerce esta necesidad la noticia que publicó en 2014 The Guardian revelando que el espionaje británico había pinchado las webcams de millones de usuarios de Yahoo. Igual de reveladora la afirmación de Assange caracterizando a los periodistas que cubren seguridad nacional como un "nuevo tipo de refugiados". Debe condenarse la recolección masiva y sistemática de datos personales de "gente inocente", comprometiendo frecuentemente la información personal íntima. Los sistemas de vigilancia masivos e indiscriminados son una interferencia seria con los derechos fundamentales de los ciudadanos. Es por ello que parecen muy tibias algunas respuestas por parte de instancias internacionales o la propia Unión Europea, publicitando como "gran epopeya" la Sentencia del Tribunal de Justicia UE en 2014 que juzgó como ilegal la Directiva del año 2006 por las que las compañías telefónicas podían guardar información de ciudadanos durante dos años. Es sabido, que, derogada la Directiva, prevalecen las legislaciones de los Estados miembros hasta que no se apruebe una nueva norma obligatoria y vinculante de la Unión Europea.

Todavía no somos conscientes del valor de nuestros datos, especialmente los médicos. El precio de nuestros datos genéticos será incalculable en el futuro, cuando los hayamos vendido por un bonito dibujo del mismo enmarcado, con la finalidad de su compra

[6] Otros lugares similares: Du Pont Fabros (cerca de Chicago); Supernap (MICROSOFT) en las Vegas; Microsoft Data Centers (en San Antonio –Texas- y Quincy –Washington); Phoenix One (Phoenix –Arizona); Microsoft Data Center (Dublín –Irlanda-); Next Generation Data Europe (Newport –Gales-), etc.: XL Semanal, nº 1366, del 29 de diciembre de 2013 al 4 de enero de 2014.

online, y las empresas o entidades aseguradoras los obtengan para sus fines (por ejemplo, la no contratación por la propensión de sufrir determinadas enfermedades según nuestro código genético), pues ahora ya muchos de nuestra información más íntima la cedemos, tal vez en un supermercado a cambio de una toalla. Seguramente la explicación de que otras empresas que los compran (obteniendo datos como el nivel adquisitivo, estilos de vida o gustos –según las compras efectuadas-), nos envíen ofertas a casa "a la carta" para nuestra sorpresa, sin haber realizado una suscripción previa (viajes, ropa, servicios sanitarios, etc). ¿Han hecho suficientes esfuerzos las Instituciones Públicas para que los ciudadanos estén debidamente informados? ¿Son conscientes los ciudadanos de esta realidad?

Estrechamente relacionado con lo anterior se encuentra el manido y polémico debate sobre la utilización de pasaportes biométricos y otros controles en los aeropuertos (como la utilización de escáner), algunos de los cuales incluso podrían ocasionar daños a nuestra salud, además de no asegurar su efectividad. El pasaporte biométrico – que incorpora un chip electrónico con datos personales, imágenes faciales y huellas digitales – está en camino de convertirse en un requisito previo global para viajes. Es muy importante que los datos biométricos sean sólo conservados en el pasaporte y no en bases de datos externas, pero hasta ahora no hay regulaciones internacionales que lo garanticen. Además, se ha demostrado que los datos en los chips son fáciles de copiar y que se puede portar un pasaporte con su verdadero nombre y foto impresos en las páginas, pero con un chip con información diferente clonada del pasaporte de algún otro. El propio Parlamento Europeo hizo públicos errores y fraudes a través de los mismos. A todo ello se suman otro importante interrogante: ¿qué otros datos podría contener? Podría ser el inicio de una desmedida cesación de información incontrolada de todos los viajeros.

La "apropiación" de los datos de los ciudadanos ha ido *in crescendo* en la propia Unión Europea. Por poner algún ejemplo, lo acontecido con la Directiva relativa a la utilización de los datos de los registros de los nombres de los pasajeros (PNR - *Passenger Name Record*-) por las compañías aéreas que hubieran efectuado vuelos entre la UE y terceros países. En un principio fue suspendida su aprobación (a pesar de haber sido propuesta ya por la Comisión en noviembre de 2007), tal vez motivada por el duro Dictamen del Supervisor Europeo de Protección de Datos. Sin embargo, la jurisprudencia de un TJUE que en gran medida está avalando la normativa, las lagunas legales y la posición general de la Unión Europea en esta materia, dirigidas a establecer de manera progresiva un control absoluto de los ciudadanos (STJUE de 17 de octubre de 2013 –por poner un ejemplo-), hacía presagiar su inminente aprobación conseguida en abril de 2016 como Directiva 2016/687, aunque no ha pasado desapercibida por numerosos juristas (CATALINA BENAVENTE: 2016; GARCÍA ROMERO: 2016), incluso criticada desde diferentes ámbitos, entre otras razones por lo relativo al número de datos objeto de transmisión y al período de conservación de los mismos (excesiva y desproporcionada).

Todos los imperios, desde Persia y Roma, hasta Venecia, la Francia de Luis XIV, la China imperial y EEUU, han vigilado a sus ciudadanos de un modo u otro. Lo revelador, por lo tanto, no es que EEUU vigile y espíe a sus propios ciudadanos ya los

ciudadanos de otros países; lo revelador es que los demás gobiernos hagan como si no supieran nada. Lo revelador, también, es que las personas de a pie no sospechen en lo más mínimo que los espían. No se trata simplemente de una cuestión de cantidad y calidad del espionaje, sino que se trata de la naturaleza misma de nuestras sociedades modernas comparadas con las antiguas.

¿Cuál es su instrumento legitimador? ¿Qué ha hecho mella en los ciudadanos para permitir esta sistemática vulneración de derechos? Sin duda los elementos a destacar como favorecedores han sido el desconocimiento y el miedo. Es cierto que la inseguridad nos afecta a todos, inmersos como estamos en un mundo fluido e impredecible de desregulación, flexibilidad, competitividad e incertidumbre endémicas (BAUMAN, 2003: 169). No obstante, debe distinguirse entre la "globalización de los riesgos" de la "globalización del miedo" (ORDÓÑEZ, 2006: 96). En muchas ocasiones es la propia sociedad la que construye las nociones de riesgo, amenaza, peligro, y genera unos modos de respuesta estandarizada, reactualizando ambos, nociones y modos de respuesta, según los diferentes períodos históricos (REGUILLO, 2000: 65) (BECK, 2003: 16) (BECK, 1998) (GIDDENS: 2000).

Y es que, si bien diversos indicios parecen indicar un retorno de la "Realpolitik" y del "Estado Guardián Hobbesiano", en nuestra época ya no se trata tanto de controlar los territorios mediante el terror, como de gestionar, administrar, dosificar hábilmente el terror que el sistema mismo produce, de manera que la situación tome, como por añadidura, el curso deseado. Muchos medios de comunicación han ayudado de forma notable a la difusión y ampliación de este sentimiento, fruto de las audiencias o de otros intereses (emprender o mantener un ejército en una guerra, promover un proyecto legislativo que limita la inmigración extranjera, motivar una ola de popularidad en época de elecciones, etc). Su papel en relación con los hechos no se reduce a su teórico papel de comunicadores (la sustracción de información, la forma de presentar las noticias y las imágenes), en el advenimiento de lo que BERICAT ha denominado como "sociedad de la infocomunicación" (BERICAT, 1996: 100).

Así, ante el "miedo", muchas veces manufacturado, se legitiman numerosas políticas como la intromisión en qué y a quién escribimos o llamamos, o la instauración de legislaciones que permiten limitar –e incluso en casos extremos conculcar–, los derechos procesales y civiles, y recortar libertades, incluida la de expresión. Un ejemplo lo ha constituido la ley ley antiterrorista estadounidense "Patriot Act" (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstructu Terrorism Act of 2001), aprobada en el año 2001, en respuesta a "una amenaza de carácter y origen indefinidos" que sin embargo se la quiso convertir "en un símbolo que convenciera a los ciudadanos de que el Gobierno Federal estaba completamente decidido a volcarse en la lucha contra el terrorismo (BRUCE ACKERMAN, 2007: 12). Ya no era necesaria la autorización judicial para que el FBI vigilase la correspondencia y las comunicaciones a través de Internet o por teléfono, y se permitía a la policía detener a extranjeros residentes sin necesidad de formular cargos contra ellos durante siete días, o la creación de Tribunales militares de excepción para juzgar a ciudadanos extranjeros sospechosos de participar en actividades terroristas o de poner en peligro la seguridad nacional.

Gran Bretaña, siempre "caballo de troya" de la estrategia USA (operando como directorio fáctico de la subalternidad europea), aprobó una ley sobre seguridad, crimen y antiterrorismo (*Antiterrorism, Crime and Security Act*) en 2001 cuya vigencia expiró en 2004, que supuso la derogación del art. 5 de la Convención Europea de los Derechos Humanos, que garantiza el derecho a la libertad y prohíbe la detención sin proceso judicial. De esta manera, ciertos sospechosos de terrorismo podían ser detenidos en el Reino Unido sin que la policía tuviera que ponerlos a disposición judicial, lo que desde un punto de vista jurídico venía a significar la revocación del derecho de *habeas corpus* reconocido en Inglaterra desde 1679. De similar talante fueron las medidas adoptadas por otros países de la Unión Europea, y las recombinaciones de alianzas o *partnership* entre los diversos Estados europeos según las cambiantes coyunturas en este ámbito.

¿Qué ha sido del Estado de Derecho? ¿Qué ha sido de los Derechos Fundamentales? ¿Qué ha ocurrido para llegar a crear artificios en un "limbo legal", con personas recluidas indefinidamente y sin asistencia jurídica en Guantánamo y en otros centros secretos de detención? (LOREDO, 2011). Se trata de una reedición del "derecho penal del enemigo": un híbrido de derecho penal y bélico que no necesita hechos para decretar la punibilidad y que permite usar medios impropios de un Estado de Derecho como la retención prolongada de sospechosos, las "presiones físicas moderadas y la licencia para 'actuar' más allá por razón de Estado". ¿Qué obliga su mantenimiento desde que, después del clamor generalizado del que se hizo eco, en enero de 2009 el Presidente Barack Obama ordenara su cierre en el plazo máximo de un año?

A inicios de junio de 2015 puede constatarse cómo expirada la vigencia de la Patriot Act, luego de sucesivas prórrogas, y sin una decidida toma de posición contraria a la misma, si no se consigue de nuevo mantenerla en vigor o con enmiendas, hay un enorme interés, más o menos disimulado según el partido político, en legislar una versión "soft" de la misma a la vez que el país galo, fruto del denominado "Efecto Charlie Hebdo", pondrá en marcha la norma que podríamos calificar como "Patriot Act Francés". En esta situación, ¿cómo pueden las democracias recurrir a estos medios sin destruir los valores que defienden?, ¿cómo pueden recurrir al mal menor sin sucumbir al mayor? (IGNATIEFF, 2004). La novela "1984" de George Orwell escrita en la primera mitad del siglo XX deja de ser una fantasía o ficción distópica en los Estados Unidos, al conceder al Gobierno poderes desorbitantes de poder para vigilar, registrar y detener. El argumento es anteponer la seguridad nacional a la libertad individual. Pero, ¿con ello además podemos hablar de garantizar la seguridad nacional? La seguridad total es una utopía, y quien crea eso va a verse frustrado y, además, habrá pagado el falso precio que comporta el recorte de derechos y libertades, que, una vez perdidos, no suelen recuperarse más. Cabe recordar en este punto la célebre frase de Benjamín Franklin, "quien prima la seguridad sobre la libertad no tiene derecho ni a la una ni a la otra".

Los Estados más decididos en el reconocimiento y protección de los derechos fundamentales a la vida y a la libertad prevén siempre alguna limitación para los casos en que el orden social y político se vea seriamente amenazado, cuya previsión no es un mero adorno del texto constitucional. Llámese estado de guerra, de excepción, los gobiernos asumen en estas situaciones poderes exhorbitantes, (situaciones que ellos

mismos deciden calificar de "extraordinarias"), una de cuyas consecuencias ha sido el reforzamiento de los poderes presidenciales frente al poder legislativo, e incluso muchas decisiones no pasan ya por los resortes parlamentarios. Sin embargo, y de todo este elenco de medidas y a pesar de los graves atentados de la última mitad del siglo XX y de principios del siglo XXI, con Nueva York, Madrid, Londres y París a la cabeza, no termina de consolidarse una postura internacional homogénea sobre cómo combatir el terrorismo y, mucho menos, sobre su definición y las causas que lo generan.

Es cierto que Internet ha supuesto un factor de incremento de formas de criminalidad, al potenciar la difusión de sabotajes, virus y abordajes a los sistemas por parte de un número imprevisible e incontrolable de *piratas informáticos* (*Hackers*). Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos: la intimidad, la imagen, la dignidad y el honor de las personas, la libertad sexual, la propiedad intelectual e industrial, el mercado y los consumidores, la seguridad nacional y el orden público. No obstante, existe una evidente dificultad para determinar la responsabilidad jurídica en un medio, como el de Internet, en el que existen diferentes operadores que concurren en la cadena de comunicaciones: el proveedor de la red, el proveedor de acceso, el proveedor de servicio y el proveedor de contenidos. Este problematismo se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos con legislaciones, a su vez, diferentes.

En la doctrina francesa se ha aludido al fenómeno de "*délocalisation*" de Internet, para hacer hincapié en los problemas jurídicos que plantea establecer el Derecho aplicable a actuaciones realizadas en una red planetaria sin "localización" geográfica precisa y determinada. Así, Internet plantea una preocupante paradoja, que deriva de su eficacia global e ilimitada para atentar contra bienes y derechos, y la incapacidad para descubrir la criminalidad informática por las dificultades que entraña *descubrirla, probarla y perseguirla*. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy deberían plantearse a los ordenamientos jurídicos nacionales y al orden jurídico internacional (RICOY CASAS, R.: 2014).

También es cierto y fundado el temor a los riesgos y amenazas en torno a las denominadas "infraestructuras críticas" (Centrales y redes de energía; Tecnologías de la información y las comunicaciones; Sistema Financiero y Tributario -por ejemplo, banca, valores e inversiones-; Sector sanitario; Espacio; Instalaciones de Investigación; Alimentación; Agua -embalses, almacenamiento, tratamiento y redes-; Transportes -aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico-; Industria Nuclear; Industria Química; Administración -servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales-). Como ejemplo de ataque, el caso Estonio a finales de abril de 2007, y como ejemplos de prevención, los simulacros efectuados por la Unión Europea, y las normas y medidas tomadas de manera creciente por incidentes dirigidos contra diferentes organismos de la Administración Pública, cada vez también sobre elementos más críticos, especialmente con la generalización e implantación también de las denominadas "Smart Cities" (RICOY CASAS: 2016).

Como en su momento expresó Snowden, nadie debe hackear infraestructuras críticas para la vida como hospitales y centrales eléctricas, pero además, tenemos que reconocer que las leyes nacionales no van a resolver el problema de la vigilancia indiscriminada. La prohibición en Burundi, no va a detener a los espías en Groenlandia. Necesitamos un foro mundial, y la financiación global, comprometida con el desarrollo de normas de seguridad que hagan cumplir nuestro derecho a la intimidad no a través de la ley, sino a a través de la ciencia y la tecnología. La manera más fácil de asegurar que las comunicaciones de un país sean seguras es fijarlo en todo el mundo y que se traduzca en mejores estándares, mejor criptografía, y una mejor investigación.

También debe tenerse en cuenta la contribución de Internet a forjar una ciberciudadanía, como forma de ciudadanía internacional y cosmopolita, se ha visto confirmada por numerosísimos fenómenos. La actitud solidaria puesta de manifiesto en la concienciación y protesta de miles de cibernautas contra la pena de lapidación impuesta a mujeres nigerianas, acusadas de supuestos adulterios; la difusión de una consciencia crítica planetaria sobre los riesgos de la globalización; la protesta respecto a la intervención bélica, al margen de la ONU en Irak; el 15-M, etc, representan experiencias elocuentes de la conformación de ese universo ciberciudadano. Por ello, se ha indicado que preguntarse sobre si Internet es buena o mala para la democracia, "parece casi ridículo" (VALLESPÍN, 2003). La Red, en definitiva, puede ser el principal cauce para promover una participación política más auténtica, plena y efectiva en las democracias del siglo XXI, en términos de ciberciudadanía; o para degenerar en un fenómeno de colonización y control de la vida cívica, quedando degradada en versiones indeseables de "ciudadanía.com".

III.- LA CONSTATACIÓN DE LA CRISIS DEL ESTADO-NACIÓN PARA HACER FRENTE A LOS RETOS DE GOBERNABILIDAD DE LAS SOCIEDADES EN LA ERA GLOBAL. LA NECESIDAD DE UNA GOBERNANZA GLOBAL

La política ha de considerarse como una práctica, proceso o actividad orientada a la regulación del conflicto y a la consecución de objetivos colectivos, siendo su resultado la adopción de decisiones que obligan a los miembros de la comunidad (ARENDT, 1992). La ciencia política nos permite descubrir la existencia de una constante a lo largo de toda la historia humana: la necesidad de la política, la dependencia radical de la misma, su inevitabilidad. Y ello porque todas las comunidades humanas, incluso las más simples y primitivas, han necesitado para su permanencia y viabilidad de un poder capaz de gestionar el conflicto (presente en todas las sociedades).

Hoy en día, y a pesar de las transformaciones tan gigantescas experimentadas por la humanidad, o quizás por ello mismo, se sigue dependiendo de la política, a quien se le formulan más demandas que en ninguna otra época, y a la que se le hace responsable del mayor número de asuntos y tareas jamás demandados con anterioridad. Es más, en esta coyuntura internacional, en la que se acumulan los llamados problemas y crisis de alcance global –y frente a los cuales se constata la incapacidad y límites del Estado-

http://revista.jacobea.edu.mx/
ISSN 2007-3798

nación tradicional-, exigimos soluciones globales, esto es, gobernabilidad mundial, que no es otra cosa más que acierto a la hora de gestionar el conflicto a escala planetaria.

Existe una coincidencia general a la hora de calificar el momento histórico que atraviesa la humanidad. Asistimos, ciertamente, a una aceleración de la historia (técnica, del cambio social, del ritmo vital…) que, lejos de reducirse, cada vez se incrementa más, razón por la cual algunos autores (MAALOUF, 2009) prefieren recurrir a otra noción que refleja mejor el ritmo de los acontecimientos de nuestro tiempo: "la instantaneidad". Al mismo tiempo tienen lugar transformaciones radicales que afectan a todos los ámbitos significativos de las sociedades humanas: a la ciencia y tecnología, a las comunicaciones, a las configuraciones geoeconómicas y geoestratégicas, a la cultura, a los distintos regímenes, a la demografía y, en fin, a los propios valores. Como consecuencia de todo ello se producen tensiones y rupturas que interactúan y se refuerzan entre sí, originando nuevas perturbaciones y turbulencias en el seno de nuestras sociedades. Es probable que estemos viviendo "momentos de apertura de la historia" (CLEVELAND, 1993). El avance general de la globalización conduce, además, y de manera inexorable, a la aparición de la política mundial postinternacional y policéntrica (ROSENAU, 1990, 2006), originando en las relaciones internacionales –y como consecuencia de la interdependencia y la interpenetración de las sociedades- una serie de mutaciones espectaculares.

El proceso de mundialización y de integración supraestatal en curso nos descubre que estamos justamente atravesando el umbral de una nueva era, la era postmoderna y posthobbesiana (SCHMITTER, 1992), la era postwestfaliana y postinternacional (ALBROW, 1996), la era global (HELD, 2006). Las instancias supranacionales y mundiales apuntan y asoman, y por la fuerza de los hechos, en el horizonte político del Planeta y, en este sentido, la llamada revolución mundial está propiciando nuevas formas y estructuras políticas e institucionales, nuevas formas e imágenes de gobernabilidad, más amplias, integradoras y globalizadas. El mundo que ahora comienza se caracteriza por esa tendencia creciente (fruto, a su vez, de la necesidad) a crear una estrecha interconexión entre lo local, lo nacional y lo global, produciéndose al mismo tiempo un gradual desbordamiento y perforación del sistema de soberanía estatal.

Se impone, pues, un cambio de paradigma jurídico y político para hacer frente a esta nueva realidad (territorialidad) global y restablecer la autoridad. Es preciso gobernar la globalización (HELD y MCGREW, 2006) para, así, poder dar respuesta a cuestiones tan fundamentales para la seguridad y el bienestar de las sociedades humanas como, por ejemplo, quién o quiénes toman realmente las decisiones y ante quiénes estos mismos han de responder y rendir cuentas (cómo y dónde resituar la *accountability* en la era global). Urge, en este sentido, buscar alternativas razonables al estatismo político imperante en nuestras sociedades.

El espectacular ensanchamiento actual de los espacios económicos, sociales y culturales ha de verse acompañado de una similar amplitud respecto de los espacios jurídico-políticos. Y, en este sentido, los Estados deben ir cediendo progresivamente parcelas de su soberanía (de algunas ya se han despojado por la fuerza de los hechos), y

vinculándose simultáneamente a normas de derecho internacional y a la decisión y veredicto de la justicia internacional. También se debe ir despejando el camino que conduce a la creación de Estados unidos de ámbito regional-continental como paso previo y condición necesaria -en nuestra opinión- para la ulterior unión mundial. La historia demuestra que los procesos de unificación -que suelen ser contagiosos- se han ido realizando a través de círculos concéntricos y mediante sucesivas etapas.

Es preciso, pues, iniciar una amplia reflexión acerca no sólo del sentido y significado del Estado en la era actual, sino también acerca de sus funciones y papel a desempeñar en el nuevo contexto de gobernanza multinivel, y de una sociedad sometida al doble proceso de globalización y de reafirmación de los hechos identitarios, de integración supraestatal y de descentralización intraestatal. ¿Qué habrá de compartir o, incluso, ceder a las unidades o niveles políticos tanto subnacionales como supranacionales o mundiales? Y también: ¿qué habrá de compartir con el mercado, con la sociedad civil, con las mil y una organizaciones privadas dispuestas a co-gobernar y a colaborar en la doble tarea de gestionar el conflicto y generar oportunidades en el seno de nuestras sociedades, y conforme al emergente paradigma de la gobernanza?

Se trata, pues, de una propuesta que se sustenta en una concepción y ejercicio del poder político inequívocamente democrático, plural, policéntrico, multilateral, federal y multinivel; lo que significa una distribución del poder entre todas las unidades políticas existentes en la actualidad (entes locales, regiones políticas o estados federados, Estados nacionales, bloques de Estados o regiones continentales), las cuales serán compatibles con ese nuevo nivel de poder a constituir: el mundial. Puede que sea un grave error no asumir que nos hallamos en un periodo histórico que reclama la revisión y puesta al día de nuestra disciplina; y, en este sentido, es probable que haya llegado el momento para impulsar, por parte de la comunidad científica, una revolución –para utilizar el concepto y esquema kuhniano- dentro de la disciplina, a fin de dar paso a un nuevo paradigma capaz de dar cuenta de las exigencias y demandas de un modelo de gobernabilidad global, interdependiente, multinivel y multilateral.

Este enfoque global de lo político, esta propuesta de transitar de la teoría del Estado tradicional a la teoría política de la era global, necesariamente va a tener otras consecuencias. En efecto, y partiendo de la idea de que a los politólogos nos correspondería –y en el nuevo contexto de unas sociedades necesitadas de nuevos modelos y arquitecturas de gobernabilidad- asumir la función de emprendedores y agentes del cambio en el ámbito sociopolítico e institucional, habría que proceder, por ejemplo, a un reforzamiento de la teoría política normativa. En todo caso, debe reclamarse en consecuencia una ciencia política postestatal e internacional, o si se prefiere, una cosmopolitología acorde con un escenario cosmopolita y con el advenimiento de la era global. La propia cooperación transfronteriza es un ejemplo que justifica los esfuerzos por cambiar la visión tradicional del Estado (RICOY CASAS y ROJO SALGADO: 2015).

La reflexión anterior nos sugiere, a su vez, la necesidad de una recuperación, o quizás una reformulación, de dos de los campos de especialización temática de la ciencia política: el institucionalismo y las relaciones internacionales. Y ello porque precisamos

de una ciencia política que se ocupe de esos nuevos modelos y escalas de arquitectura constitucional demandados por el nuevo escenario global; un nuevo constitucionalismo más allá del ámbito y la idea del Estado-nación tradicional. Necesitamos de un nuevo institucionalismo, que nos recuerde que las instituciones importan (ellas disciplinan y regulan nuestras conductas, a la vez que orientan, canalizan y generan expectativas), y que más allá del Estado hay vida y hay política; que nos recuerde que es preciso tomarse en serio la institucionalización de un gobierno mundial (HABERMAS, 2004), incluyendo la tarea de definir y asignar un reparto y una división multinivel de poderes y competencias, desde lo local a lo global, y conforme a las exigencias del principio federal de la subsidiariedad.

IV.- ALGUNAS CONCLUSIONES

Nadie discute las grandes ventajas de un sistema informático que permite la eficaz persecución de la delincuencia organizada, pero que por el contrario se discuten las insuficientes garantías jurídicas y técnicas tanto para preservar los derechos fundamentales de los ciudadanos a través del adecuado control judicial, como para garantizar la destrucción de datos no necesarios para un Tribunal, la exactitud de los archivos que se pongan a disposición judicial, y a la seguridad en la custodia y funcionamiento del sistema que debería de estar asignado a un órgano del Estado y no a una empresa externa. En los casos de interceptación de las comunicaciones legalmente establecidos puede justificarse la invasión a los derechos fundamentales que presupone la misma, siempre que haya un equilibrio racional entre los derechos limitados y las conductas delictivas perseguidas, según el principio de proporcionalidad. No obstante, si se saltan los mecanismos legalmente establecidos, aunque sea promovida por gobiernos en su celo de garantizar la seguridad en casos tan graves como terrorismo o bandas organizadas, existe una indefensión de dichos derechos por parte del individuo y aumenta enormemente la posibilidad de un uso pernicioso de la información obtenida, al faltar un control legal, máxime si las intervenciones se realizan de forma arbitraria o indiscriminada.

El desarrollo legislativo de la materia tiene ambigüedades, errores y omisiones que debieran ser revisados y subsanados. En España, es criticable que el mismo se realice principalmente en leyes de menor orden a las adecuadas para legislar derechos fundamentales, que deben tener reserva de ley orgánica tal y como se recoge en el artículo 81 de la CE, lo que obliga a un mayor consenso necesario al regular materias tan sensibles. Asimismo, la insuficiencia de las disposiciones de la LECrim para cumplir los compromisos internacionales en esta materia ha obligado a la jurisprudencia a complementar las mismas. Además, se ve una clara tendencia a implantar instrumentos de control de las comunicaciones para infracciones de menor entidad, como las descargas particulares de contenido protegido con copyright, vulnerando el principio de proporcionalidad. Asimismo, se debería legislar de forma muy específica y restrictiva -y velar con especial celo su cumplimiento- el registro, protección y uso de información por corporaciones que, por su ingente cantidad de usuarios y el registro intensivo de sus transacciones al usar el sistema, tengan potencial de vulnerar de forma grave, masiva y arbitraria los derechos mencionados, como buscadores Web, redes

sociales e ISPs. Y bajo ninguna circunstancia se debería permitir el análisis o minería de datos con fin distinto del estricto funcionamiento del sistema ni, lo más aberrante, venderlos a terceras partes (CASTELLANO y SANTAMARÍA, 2013).

La dimensión internacional de estas problemáticas junto con otras como la seguridad alimentaria, o las políticas medioambientales, por poner algunos ejemplos, obligan a hacer un esfuerzo por gobernar la globalidad, las cuestiones de dimensión y de implicaciones internacionales, mucho más allá de los resortes de los parlamentos nacionales. Para ello ha de tenerse en cuenta a una auténtica pléyade de actores, redes de actores, cuya concertación y consenso produzcan un cambio de paradigma jurídico y político sin el cual no será posible esta gobernabilidad. Es por ello el momento de la política, es protagonista principal en la búsqueda de estas respuestas que demanda la comunidad internacional.

V.- BIBLIOGRAFÍA

ALBROW, M.: (1996) *The Global Age*. Polity Press. Cambridge.

AÑOVER, J.: (1984*) Echelon y Enfopol nos espían*, 2001 en http://www.nodo50.org/altavoz/echelon.htm (fecha de consulta: 12/01/2014).

ARENDT, H. (1992): *¿Qué es la política?* Barcelona, Paidós.

ATTINÀ, S.: (2001) *El sistema político global.* Barcelona, Paidós.

BALLESTEROS, J.: (1995) *Ecologismo personalista*, Tecnos, Madrid.

BAUMAN, Z.: (2003) *Comunidad. En busca de seguridad en un mundo hostil*, Siglo XXI, Madrid.

BECK, U.: (1998) *¿Qué es la globalización?* Paidós. Barcelona.

BECK, U.: (1998) *La sociedad del riesgo: hacia una nueva modernidad*, Paidós, Barcelona.

BECK, U.: (2003) *Sobre el terrorismo y la guerra*, Paidós, Barcelona.

BECK, U.: (2005) *La mirada cosmopolita o la guerra es la paz,* Paidós. Barcelona.

BERICAT ALASTUEY, E.: (1996) *La sociedad de la Información: tecnología, cultura, sociedad*, en REIS, nº 76.

BOHMAN, J.: (2007) *Democracy across Border,* Cambridge (Massachusetts), The MIT Press.

BRUCE ACKERMAN: (2007) *Antes de que nos ataquen de nuevo*, Península, Barcelona.

CASTELLANO OSUNA, M.A. y SANTAMARÍA HERNÁNDEZ, P.D.: (2013) *El control del ciberespacio por parte de gobiernos y empresas,* en Seguridad. Cuaderno Red de Cátedras Telefónica, No. 9. Diciembre de 2012. Número extraordinario.

CATALINA BENAVENTE, M.A.: (2016) "La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos en la lucha contra el terrorismo y la delincuencia grave", en Diario La Ley, nº 8801.

CLEVELAND, H.: (1993) *Birth of a New World: An Open Moment for International Leadership*. Jossey-Bass. San Francisco.

DEUTSCH, K. W.: (1981) *Las naciones en crisis.* F.C.E. México.

DÍAZ BERMEJO, G.: (2009) *SITEL. La gran oreja del Gobierno no tiene suficientes garantias jurídicas*, en Noticias Jurídicas.

DROR, Y.: (1994) *La capacidad de gobernar*. Informe al Club de Roma. Galaxia Gutenberg/Círculo de Lectores. Barcelona.

FUKUYAMA, F.: (2004) *La construcción del Estado.* Ediciones B. Barcelona.

GARCÍA ROMERO, S.: (2016) "Nuevo marco jurídico europeo: novedades conocidas y otras no tan conocidas", en Diario La Ley, nº 8690, 3.

GARDINER, N.: (2005) *Apoyo a las medidas antiterroristas de Gran Bretaña*, *Colaboraciones (Grupo de Estudios Estratégicos)* nº 515.

GIDDENS, A.: (2000) *Un mundo desbocado. Los efectos de la globalización en nuestras vidas*, Taurus, Madrid.

GLASER, D.: (1997) "La teoría normativa", en MARSH, D. y STOCKER, G. (eds.), *Teoría y métodos de la ciencia política.* Alianza. Madrid.

HABERMAS, Jürgen (2004): "De la política de poder a la sociedad civil mundial", en *Tiempo de transiciones,* Madrid, Trotta.

HELD, D.: (1997): *La democracia y el orden global. Del Estado moderno al gobierno cosmopolita.* Paidós. Barcelona.

HELD, D.: (2005) *Un pacto global*. Taurus. Madrid.

HELD, David & MACGREW, Anthony: (2006) "Introduction", en HELD, David & MACGREW, Anthony (Ed.) *Governing Globalization,* Cambridge (UK), Polity Press, págs. 1-21.

HELD, David: (2010) *Cosmopolitanism. Ideals and Realities,* Cambridge (UK), Polity Press.

HUEGLIN, Thomas O.: (1999) « Le fédéralisme d'Althusius dans un monde post-westphalien », en *L'Europe en Formation,* núm. 312, págs. 27-54.

IGNATIEFF, M.: (2004) *El mal menor, ética política en una era de terror*, Taurus, Madrid.

LOREDO COLUNGA, M.: (2011) *El cierre de Guantánamo. El difícil equilibrio entre voluntad política, legalidad y opinión pública*, en InDret Revista para el análisis del derecho.

MAALOUF, A.: (2009) *El desajuste del mundo. Cuando nuestras civilizaciones se agotan*. Alianza Editorial. Madrid.

ORDÓÑEZ, L.: (2006) *La globalización del miedo*, Revista de Estudios Sociales, nº25.

PANEBIANCO, Angelo: (1996) "La dimensión internacional de los procesos políticos", en G. Pasquino *et ali Manual de ciencia política*. Alianza Editorial. Madrid.

PEÑA, J.: (2010) *La ciudad sin murallas. Política en clave cosmopolita*. El Viejo Topo. Barcelona.

POGGE, T.: (2005) "A cosmopolitan perspective on the global economic order", en G. Brock & H. Brighouse (eds.) *The Political Philosophy of Cosmopolitanism.* Cambridge U. P. Nueva York.

REGUILLO, R.: (2000) *Los laberintos del miedo. Un recorrido para fin de siglo,* Revista de Estudios Sociales, nº5, Facultad de Ciencias Sociales-Fundación Social, Bogotá.

RICOY CASAS, R. M.: (2014) *Ciberespacio, Espionage y Seguridad internacional: nuevos desafíos para la gobernanza,* en el VII Congreso Internacional de la Asociación Portuguesa de Ciencia Política APCP, celebrado en la Facultad de Economía de la Universidad de Coimbra (Portugal) del 14 al 16 de abril de 2014.

RICOY CASAS, R. M.: (2016) *La Smart City Vigo*, ponencia defendida en el VII Congreso Internacional en Gobierno, Administración y Políticas Públicas, celebrado en Madrid, del 3 al 5 de octubre.

RICOY CASAS, R.M. y ROJO SALGADO, A.: (2015) *La cooperación transfronteriza: de la separación al reencuentro… ¿y a la integración?*, ponencia defendida en el XII Congreso Internacional de Ciencia Política y de la Administración celebrado en San Sebastián del 13 al 15 de julio de 2015, en la Universidad del País Vasco.

ROJO SALGADO, A.: (2000) *Globalización, Integración Mundial y Federalismo*, en Revista de Estudios Políticos.

ROSENAU, J.N.: (1990) *Turbulence in World Politics: A Theory of Change and Continuity*. Brighton. Harvester.

SANSÓ-RUBERT PASCUAL, D.: (2004) "Seguridad versus libertad: El papel de los servicios de inteligencia", en Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol, Universidad de Valencia, nº48.

SCHMITTER, P.: (1992) "La Comunidad Europea como forma emergente de dominación política", en J. Benedito y F. Reinares (eds.) *Las transformaciones de lo político*. Alianza. Madrid.

SORROZA BLANCO, A.: (2004) "La UE y la lucha contra el terrorismo: del 11-M al 7-J", en Análisis del Real Instituto Elcano (ARI) nº 92.

VALLESPÍN, F.: (2003) *Democracia e Internet*, *El País*, 12 de abril.