Democracia y protección de datos*

Stefano Rodotà

1. La democracia se define no sólo como «gobierno del pueblo», sino también como «gobierno en público». De esta manera, la transparencia es un elemento fundamental del proceso democrático, de la corrección de la vida pública en su conjunto. «La luz del sol es el mejor desinfectante», escribió Luis B. BRANDEIS, importante juez del Tribunal Supremo de los Estados Unidos.

¿Es posible que la defensa de la privacidad conviva con esta idea de democracia? No se trata de una pregunta marginal, pues se refiere a un aspecto cada vez más importante de la posición del ciudadano en el sistema político-institucional. ¿Cómo se entrelazan la esfera pública y la privada? ¿Cuál debería ser en esta materia la relación entre la libertad del individuo y las intervenciones del Estado?

Hay una manera extrema de enfrentarse con este problema, propuesto recientemente con fuerza, sobre todo con el argumento de la necesidad de adoptar medidas para luchar contra el terrorismo. Se dice que el ciudadano que no tiene nada que esconder, no tiene nada que temer. Este ciudadano, entonces, no tendría razón alguna para estar preocupado en caso de que el Estado recopilase toda la información posible que se refiriese a él.

Pero el «hombre de vidrio» es una metáfora nazi que refleja la idea de un Estado que puede adueñarse por entero de la vida de las personas, que frente a sí no tiene ciudadanos, sino súbditos. Las consecuencias de este

---

* Traducción revisada por José Luis PIÑAR MAÑAS.

planteamiento son dramáticas para las personas y destructivas para la democracia. En efecto, si una persona quiere preservar una esfera, aunque mínima, de privacidad e intimidad, y desea que nadie conozca ciertas informaciones sobre sí mismo, se convierte, según el Estado, en «alguien que tiene algo que esconder» y, automáticamente, en sospechoso, en «enemigo del pueblo». Se trata de una lógica típica de los regímenes totalitarios y, por tanto, contraria a la democracia.

Los regímenes democráticos actúan (o tendrían que actuar) según lógicas profundamente distintas, basando las posibles limitaciones a la privacidad en el principio democrático. En este sentido, el artículo 8 del Convenio Europeo de Derechos Humanos de 1950 es muy claro, estableciendo que sólo son admisibles las medidas de limitación que sean necesarias «en una sociedad democrática». De esta manera se establece una relación firme entre democracia y respeto de la vida privada, afirmando que las medidas que limitan esta última son legítimas sólo si superan el test de democracia. Una tutela efectiva de la privacidad se transforma, entonces, en elemento básico para que una «sociedad» pueda seguir llamándose «democrática». La idea del «hombre de vidrio» se desecha totalmente.

Pero precisamente el carácter «público» de la democracia exige un mayor análisis de esta idea. En 1964, en el caso *New York Times v. Sullivan,* el Tribunal Supremo de Estados Unidos estableció que las *public figures* gozan de una tutela de su privacidad más atenuada que la que corresponde a las personas comunes. Esto no significa que pierdan todo derecho a la tutela de su privacidad e intimidad. Como ha señalado el Tribunal Europeo de Derechos Humanos en el reciente caso de Carolina de Mónaco, la divulgación de noticias que se refieren a «personas públicas» es legítima sólo si existe «un interés público» en su conocimiento. Se define así uno de los criterios para el ejercicio del derecho de informar y ser informados y el papel de las informaciones personales en el proceso democrático.

La difusión de informaciones personales delicadas, en efecto, ha de ser considerada legítima si contribuye de manera importante a hacer posible el control por la opinión pública, y específicamente por los electores, sobre los comportamientos de hombres políticos y, más en general, de quienes desarrollan cargos públicos. La libre decisión del individuo de situarse en la esfera pública conlleva una atracción hacia tal esfera de una parte de informaciones privadas. Algo muy distinto a la supuesta obligación de todos de «desnudarse» ante el Estado u otros ciudadanos.

2. Sin embargo, para comprender enteramente la manera en que se desarrolla hoy la relación entre democracia y datos personales no es posible limitarse a este tipo de consideraciones, sustancialmente basadas en una idea de privacidad como «derecho a ser dejado solo». Recientemente se ha producido una mutación radical, de la mano de la Carta de Derechos Fundamentales de la Unión Europea, ahora incorporada al texto de la Constitución europea recientemente aprobado.

La Carta distingue entre el tradicional derecho «al respeto de la propia vida privada y familiar» y el «derecho a la protección de datos personales». El primero está mencionado en el artículo 7, que en resumen reproduce el esquema del artículo 8 del Convenio Europeo de Derechos Humanos. El segundo, recogido en el artículo 8 de la Carta, consagra el carácter autónomo del derecho fundamental, distinto del derecho a la tutela de la vida privada. Y es importante resaltar que, caso único en el entero texto de la Constitución europea, al derecho a la protección de datos personales se dedica un artículo específico también en la primera parte (artículo 51). Este nuevo derecho fundamental no puede ser enmarcado en el esquema de «ser dejado solo», sino que se concreta en la atribución a cada uno del poder de «gobernar» la circulación de las informaciones que le conciernen. Se transforma así en elemento capital de la libertad del ciudadano en la sociedad de la información y de la comunicación.

Esta distinción no es sólo un aspecto externo. El hecho de que nuestra vida se está transformando, sin duda, en un canje continuo de informaciones, y de que vivimos en un flujo continuo de datos, ha atribuido a la protección de datos una importancia creciente, desplazándola hacia el centro del sistema político-institucional y atribuyéndola una importancia creciente y autónoma. En el tradicional derecho al respeto de la vida privada y familiar se expresa sobre todo un momento que se refiere al individuo, y el poder se limita a la exclusión de interferencias ajenas: la tutela es estática, negativa. La protección de datos, por el contrario, fija normas sobre las modalidades de tratamiento de datos, se concreta en poderes de intervención: la tutela es dinámica, y sigue a los datos durante su circulación. Los poderes de control e intervención, además, no pertenecen sólo a las personas directamente interesadas, sino que son confiados a una autoridad independiente, como explícitamente se ha previsto en el artículo 51 de la primera parte y en el artículo 68 de la segunda parte de la Constitución europea. Desde esta perspectiva, la tutela no se confía sólo a la iniciativa de las personas interesadas, sino que implica permanentemente una específica responsabilidad pública. Además, la Constitución prevé la necesaria creación de una autoridad independiente sólo para la protección de datos personales, subrayando con fuerza la importancia de este nuevo derecho fundamental.

Estamos ante una nueva distribución de los poderes sociales y jurídicos. Es evidente que hemos llegado al límite de una larga evolución del concepto de privacidad, desde su definición original como «derecho a ser dejado solo» hasta el poder de controlar las informaciones que conciernen a cada uno y decidir las modalidades de construcción de su propia esfera privada. Se contribuye así, de manera importante, al proceso de «*constitucionalización* de la persona».

¿Por qué esta innovación, esencial para la posición de las personas, tiene tanta importancia cuando se aprecia desde la óptica del funcionamiento del sistema democrático? La construcción tradicional dibujaba el dere-

cho a la tutela de la vida privada y familiar según el esquema del derecho de propiedad, excluyendo el «acceso» por parte de los demás a su propia esfera privada. La protección de datos modifica esta perspectiva, y la pone casi del revés, basando el nuevo derecho en el «acceso» por parte de todos los interesados a las informaciones que los demás tienen en relación con ellos. En principio, ya no existe un «santuario» público o privado protegido de la mirada de los ciudadanos. La previsión general del derecho de acceso hace que la transparencia total de la organización social crezca, con un efecto evidente e inmediato de desarrollo de la democracia.

En efecto, es posible ejercer un control sobre todos los que disponen de informaciones, hasta el punto de que en ciertos países se reconoce incluso el derecho de acceso a los datos recogidos por los servicios secretos, aunque tal derecho deba ejercitarse por medio de la autoridad de control (así está previsto, por ejemplo, en la ley italiana). Y, dado que nuestras organizaciones sociales se basan cada vez más en la disponibilidad de información, esta novedad se concreta en la creación de un contra-poder difuso, a cuyo funcionamiento colabora la acción capilar de los individuos y los grupos y la intervención de entidades públicas (las autoridades independientes, ahora previstas en la Constitución a nivel europeo, como ya he apuntado).

El resultado puede parecer paradójico sólo a quien sigue identificando la protección de datos con el carácter secreto de las informaciones, olvidando la mutación «revolucionaria» representada por el reconocimiento a todos los ciudadanos de un poder permanente de control sobre sus propios datos, donde quiera se encuentren, que se traduce en un poder de control sobre los sujetos, sean quienes fueren, que disponen de datos personales. Éste es un proceso inédito, hasta ahora desarrollado sólo en la Unión Europea, donde es posible anunciar la creación de un nuevo «modelo» que, reforzando la esfera privada, refuerza al mismo tiempo el peso de cada uno en la esfera pública. De este modo es posible concluir que el derecho fundamental a la protección de datos personales se transforma en un elemento básico de la nueva «ciudadanía electrónica».

3. Estas consideraciones de orden general son reforzadas por análisis más específicos, que tienen sobre todo que relacionarse con Internet. Éste no es el lugar donde discutir los problemas conexos con la posibilidad de estimar Internet como el instrumento que puede marcar el cambio definitivo de la democracia representativa hacia la democracia directa. Pero es cierto que en este espacio público inmenso, el más amplio que la humanidad haya conocido, muchas son las oportunidades democráticas, y muchas, para que sean utilizadas en la realidad, requieren la protección de los datos personales.

La experiencia de estos últimos años pone en evidencia que la esfera de la política se relaciona con las tecnologías de la información y de la comunicación sobre todo en lo que se refiere al *e-government*, al desarrollo

del control sobre las personas, a las iniciativas directas de los ciudadanos. Está claro que se trata de dinámicas que se refieren a lógicas distintas: eficiencia, control, participación.

Analizando más en detalle estas dinámicas, nos damos cuenta de que a menudo a los ciudadanos se les promete un futuro lleno de eficiencia administrativa y se les oculta un presente en que los instrumentos de un control cada vez más invasivo y capilar se multiplican. Casi parece que se estén construyendo dos mundos que no se comunican, y que el *e-government,* la Administración electrónica, pueda desarrollarse sin tener en cuenta el aplastamiento contemporáneo de derechos individuales y colectivos, con la excusa de exigencias de eficiencia o de seguridad. No es casualidad que los administrados sean llamados «clientes» y se utilicen fórmulas del lenguaje de la empresa, tales como *costumer satisfaction*, convirtiendo al ciudadano en un mero consumidor de servicios.

Pero también la eficiencia puede ser víctima de esta esquizofrenia institucional. La participación del ciudadano en los procesos de *e-government,* en efecto, puede ir acompañada del registro de las distintas formas y ocasiones en que se plasma: consultas, intervenciones en procedimientos administrativos, utilización de servicios. Los datos así recogidos pueden ser utilizados para distintos fines, elaborando, por ejemplo, perfiles de ciudadanos «activos» o fichando opiniones, preferencias, orientaciones. Si este conjunto de informaciones es utilizado para actividades de control o de simple interferencia en la esfera privada, o así lo percibe el ciudadano, existe el riesgo de desincentivar la participación al objeto de evitar consecuencias no deseadas.

Concluyendo: el poder del ciudadano no se refuerza en realidad si, al mismo tiempo, se hace crecer su dependencia. No es posible construir una participación separada de un respeto firme a todos los derechos de los participantes, concretándose en una fuerte protección de datos personales. No es posible separar el tema del *e-government* del de la *e-democracy*, que se basa a su vez en una ciudadanía electrónica que comprenda la protección de los datos personales.

Pero, con exclusión de su utilización como instrumento de procedimientos más o menos formales, Internet se presenta como un espacio público de debate, de relación, de proposición, y por tanto como un momento cada vez más importante del proceso democrático en su conjunto. En esta más amplia dimensión, la protección efectiva de los datos personales es básica para que la participación efectiva de todas las personas sea posible.

Hay situaciones en las que la posibilidad de explotar las ocasiones democráticas que Internet ofrece requieren que se pueda gozar de las mismas condiciones de «invisibilidad» por tradición reservadas sólo al momento de la expresión del voto en las elecciones. Es el tema del anonimato como condición de libertad, que se presenta como condición imprescindible para la libertad de expresión, la participación política, el control sindical.

Si, por ejemplo, un refugiado político quiere utilizar Internet para denunciar las violaciones de las libertades en el país del cual ha huido, el respeto de su anonimato es imprescindible para evitar venganzas contra su familia en su patria, y, en consecuencia, para permitir que exprese libremente su opinión. Lo mismo acontece en el caso de que se quiera financiar un partido o un candidato por Internet sin por eso ser objeto de consecuencias negativas o intimidaciones. El reciente desarrollo de la actividad de control por parte de los sindicatos en lugares o empresas hostiles, sobre todo en los Estados Unidos, se explica por la posibilidad de denunciar anónimamente, por medio de Internet, acciones que violan los derechos de los trabajadores.

No es casualidad que los regímenes totalitarios ejerzan un fuerte control sobre Internet, como acaba de poner en evidencia el Informe 2004 de *Reporters sans frontières*, cuyo título es precisamente *Internet sous surveillance*. Este control se ejerce por medio de la identificación de los usuarios y el filtro de temas y argumentos. Se fichan personas y se realizan formas de censura, a menudo utilizando el argumento de la lucha contra la pornografía y la pedofilia. En contra de estas tendencias, el Tribunal Supremo de Estados Unidos ha declarado, en una sentencia del pasado mes de junio de 2004, que el *Child Online Protection Act (COPPA)* de 1998 viola específicamente la primera enmienda de la Constitución sobre el *free speech* porque prevé que, para acceder a ciertos sitios de Internet, los adultos han de registrarse o utilizar ciertos códigos.

4. Resulta evidente, de este modo, otro aspecto de la relación entre democracia y protección de datos personales. Esta protección representa una condición preventiva para poder gozar enteramente de otros derechos fundamentales, que constituyen exactamente el núcleo de las libertades democráticas.

Analicemos el artículo 8 de la Directiva europea 95/46, que prevé una regulación específica para los datos sensibles, cuyo tratamiento está en principio prohibido. Entre estos datos sensibles están mencionadas «las opiniones políticas» y la «afiliación sindical», cuya tutela reforzada, sin embargo, no deriva de exigencias de secreto. Al contrario, las opiniones políticas o sindicales no pueden ser enmarcadas en la esfera *privada:* en los Estados democráticos pertenecen sobre todo a la esfera *pública,* forman parte de las convicciones que el individuo debe poder expresar *en público*, contribuyen a formar su identidad *pública*. Dotar a estos datos de una protección específica contra los riesgos de su tratamiento es consecuencia de su posible aptitud de ser utilizados con fines discriminatorios. De aquí deriva una aparente paradoja: a estos datos típicamente públicos se les atribuye el máximo de protección *privada.* Y esto conlleva una sustancial mutación de las razones de la tutela: el fin ya no es estimar el secreto como un bien en sí mismo, sino impedir posibles discriminaciones, hacer que la igualdad sea efectiva.

En consecuencia, cambia profundamente la función sociopolítica de la privacidad, que de esta manera sobrepasa la esfera privada, confirmándose como elemento constitutivo de la ciudadanía. Y su definición, durante largo tiempo únicamente conexa al «derecho de ser dejado solo», se dilata y dirige hacia la idea de tutela global de las opciones de vida contra toda forma de control público y de estigmatización social, en un marco caracterizado por la libertad de las opciones existenciales y políticas.

Estamos frente a una perfecta correspondencia entre la regulación de tales datos sensibles y las normas constitucionales sobre la igualdad. En el artículo 21 de la Carta de Derechos Fundamentales de la Unión Europea se prohíbe expresamente «cualquier forma de discriminación que se base», entre otros casos, precisamente en «las opiniones políticas o de cualquier otra naturaleza». Para alcanzar este fin, esencial para la afirmación del valor democrático de la igualdad, es imprescindible una regulación específica y firme de esta categoría de informaciones personales.

Asimismo, y en relación con el principio de igualdad, revisten especial importancia los datos genéticos. A las «características genéticas» se refiere también el ya mencionado artículo 21 de la Carta Europea de Derechos Fundamentales, prohibiendo su utilización con fines discriminatorios, de acuerdo a la línea ya señalada en documentos internacionales tales como la Carta de Oviedo sobre la Biomedicina y la Declaración Universal sobre el Genoma Humano de la Unesco. Numerosas legislaciones, y no sólo europeas, han aceptado esta vía y excluyen la posibilidad de tratar datos genéticos para fines distintos de los que se refieren a la tutela de la salud del interesado o al desarrollo de investigaciones científicas.

Esta tendencia se está afirmando también en Estados Unidos, donde, en diciembre de 2003, el Senado aprobó la *Genetic Non-Discrimination Act,* que impide la utilización de estos datos por parte de las compañías de seguros y los empresarios. Entre las razones que han conducido a la aprobación de este proyecto de ley, cabe destacar la que deriva de la propia realidad: un tercio de las mujeres a las que se proponía someterse a pruebas gratuitas de detección de cáncer de mama se negaban, basando su negativa en el temor de que las informaciones resultado de las pruebas pudiesen ser conocidas por la empresa donde trabajaban o su compañía de seguros, con el consecuente riesgo de ser despedidas o de denegación (o imposición de condiciones muy onerosas) del contrato de seguro. Sólo una intensa protección de los datos genéticos parecía ser, por tanto, la que podía liberar a las mujeres de la «elección trágica» entre tutela de la salud y conservación del empleo o del seguro.

Concluyendo, estos ejemplos y este análisis confirman la tesis que considera la protección de datos como un derecho fundamental, que se expresa también como condición preventiva para poder ejercer de modo efectivo otros derechos y libertades fundamentales, como la libertad de expresión, la libertad de organización política y sindical, el derecho a la salud. En razón del hecho que la democracia no se refiere sólo a las nor-

mas de funcionamiento de las instituciones, sino que se expresa en las libertades y derechos fundamentales, el test de «impacto privacidad» es imprescindible para juzgar el efectivo nivel de democracia de un sistema político.

5. El panorama es más grave tras los atentados del 11 de septiembre de 2001, con un fuerte incremento en la recogida y tratamiento de datos personales para fines de policía, utilizando en particular y cada vez más los datos biométricos, en primer lugar las huellas dactilares, lo que hace posible llevar a cabo controles generales de todos los ciudadanos. Parece que transformándose en «infinita» la guerra, infinitas tengan que ser las formas de control, con una mutación de la calidad de las relaciones entre Estado y ciudadano, con profundas transformaciones de la entera organización social. No en vano, yendo más allá de la específica pretensión de las autoridades americanas de obligar a muchos visitantes extranjeros a facilitar sus huellas al entrar en Estados Unidos, se ha visto en ello una señal de una nueva definición del «normal estatuto jurídico-político de los ciudadanos en los Estados así llamados democráticos». El cuerpo se transforma en un medio para incrementar las medidas de policía, en una progresión tal que también la mente puede ser capturada por la invasión rastrera de las tecnologías de control de la vida cotidiana. Las huellas dactilares, en efecto, sólo son uno de los datos biométricos utilizados para fines de identificación y control. Y de ellos no se abusa sólo en Estados Unidos. En numerosos países son utilizados para el control de la entrada en ciertos lugares, y se quieren utilizar incluso para controlar la entrada en las aulas y comedores de los niños en las escuelas primarias.

De este modo, el cuerpo cobra nueva y mayor importancia, pues se transforma en fuente de nuevas informaciones, objeto de un nuevo *data mining*, realmente una mina abierta de donde extraer datos sin parar. El cuerpo en sí mismo se está transformando en una *password*, el carácter físico sustituye a las abstractas claves de acceso. Huellas dactilares, geometría de la mano o de los dedos o de las orejas, iris, retina, rasgos, olores, voz, firma, utilización de un teclado, manera de andar, ADN. Estos datos biométricos son utilizados cada vez más no sólo para fines de identificación o como clave de acceso a distintos servicios, sino también como elementos para clasificar de manera permanente, para controles sucesivos en el momento de la identificación o de la autentificación/averiguación, es decir, de la confirmación de una identidad.

Pero durante estos años no sólo ha crecido la presión para reducir la protección de datos personales en nombre de la lucha contra el terrorismo. También ha crecido la conciencia de la importancia de la protección de datos como aspecto básico de la libertad personal. No es casualidad que desde hace años se hable de la exigencia del *habeas data,* utilizando la fórmula del *habeas corpus,* que en la historia representa el primer reconocimiento de la libertad personal. Es la persona concreta la que necesita tu-

tela, debido a que, cuando se trata específicamente de sus datos biométricos, revela una nueva debilidad: la posibilidad que sea desarmada en pedazos. Transformándose en «múltiple» es necesario seguir pensando en el cuerpo como «uno».

«No pondremos la mano sobre ti». Ésta era la promesa de la Magna Charta: respetar el cuerpo de manera integral. Esta promesa ha de sobrevivir a los avances tecnológicos. Cualquier tratamiento de datos biométricos ha de ser juzgado en referencia al cuerpo entero, a una persona que tiene que ser respetada en su integridad física y psíquica. Esto es lo que declara expresamente el artículo 3 de la Carta de Derechos Fundamentales de la Unión Europea. Tal precepto, junto con el ya mencionado reconocimiento de la protección de datos personales como derecho fundamental, confirman que estamos ya ante la «*constitucionalización* de la persona». Ha nacido un nuevo concepto integral de la persona, a cuya proyección en el mundo corresponde un derecho fuerte de no perder nunca el poder de guardar el control total de un cuerpo que ya es, al mismo tiempo, «físico» y «electrónico».

6. Pero la libertad del cuerpo físico y electrónico queda cuestionada ante la difusión de formas de vigilancia generales, de la conservación de datos de tráfico telefónico y en la red, de las tecnologías de localización. Ya es conocido el caso de Echelon, un sistema de escucha planetaria de las comunicaciones electrónicas realizado por Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda. Estados Unidos está proyectando nuevos sistemas de control según el modelo del *Terrorism Information Awareness (TIA),* hoy sólo en apariencia abandonado. Se difunde la conservación de datos de tráfico durante periodos más o menos largos (desde seis meses hasta cinco años), haciendo posible un control capilar y la reconstrucción de relaciones y costumbres de las personas por medio de la conservación de datos que se refieren al correo electrónico, a los accesos a las páginas web, a las participaciones en *chats*. Por medio de la red telefónica móvil, o de los chips bajo la piel, las *smart tags* realizadas por medio de la tecnología de identificadores de radiofrecuencias (RFID), es posible localizar permanentemente a una persona, seguirla en sus desplazamientos: una red invisible nos acompaña, el cuerpo humano se transforma en un mero objeto en movimiento controlado por medio de tecnologías satelitales.

El cambio social está justo aquí. La vigilancia pasa de tener un carácter excepcional a ser cotidiana; de las clases «peligrosas» a la generalidad de las personas. La multitud ya no es solitaria y anónima. Las imágenes digitales, las técnicas de reconocimiento de los rasgos, permiten sacar al individuo de la muchedumbre, individualizarlo y seguirlo. El *data mining*, la búsqueda sin parar de informaciones sobre la conducta de cada uno, engendran una producción continua de «perfiles» individuales, de familia, de grupo: otra vez, la vigilancia no tiene límites.

No es entonces arbitrario analizar este conjunto de mutaciones desde el punto de vista de un modelo de Panopticon que, alejándose de su original matriz carcelaria, se aplica al conjunto de relaciones sociales. De aquí resulta de manera muy clara que la vigilancia engendra un nuevo equilibrio de poderes, configurando la constitución misma del sujeto.

El paso de una vigilancia dirigida a lo general, las recogidas de datos personales de la multitud, ya han causado la transformación de todos los ciudadanos en posibles sospechosos, frente a los poderes públicos, y la transformación de la persona en objeto, frente al sistema de empresas. Esto hace siempre más difícil trazar distinciones claras entre espacio público y privado. La conservación de datos relativos al tráfico telefónico, al correo electrónico, a la navegación en Internet, es efectuada por sujetos privados y, sobre todo, para fines de policía y justicia. Las empresas utilizan ampliamente bancos de datos públicos para sus políticas comerciales, sus estrategias con referencia a los consumidores. Al mismo tiempo, en ciertos países hay sociedades privadas que compran grandes bases de datos para ponerlas a disposición de autoridades públicas que no podrían crearlas directamente.

La creación de «naciones de sospechosos» ha sido incentivada con fuerza por las legislaciones y las prácticas legales adoptadas tras los atentados del 11 de septiembre. Se pone de manifiesto una nueva dimensión de la vigilancia que exalta el poder del Estado de obtener cualquier información personal, quien quiera la haya recogido e independientemente del fin original de la recogida. Aunque la vigilancia efectuada por los particulares siga siendo prevalente desde el punto de vista de la cantidad, y por tanto del conjunto de informaciones de que disponen, esto no implica una separación entre público y privado, pues el conjunto de datos tratados por los privados es considerado como una fuente de información a disposición de los poderes públicos.

De este profundo cambio político, social y jurídico algunos autores norteamericanos han pretendido ofrecer una interpretación «democrática». Se dice que, en el pasado, el control y la vigilancia estaban dirigidos sólo a personas sospechosas, a grupos o clases peligrosos, con un efecto de discriminacion social. Cuando se pasa a un control universal, para todos los ciudadanos, se incrementa la igualdad y, por eso, la democracia. ¿Hemos de concluir que la democracia perfecta se identifica con el control generalizado?

No creo que sea necesario rebatir esta tesis. No es una paradoja, sino un inaceptable intento de racionalizar y justificar las nuevas formas de vigilancia total.

En realidad, la vigilancia no quiere tener límites ni obstáculos a la utilización de cualquier técnica. Se adueña del espacio, físico y virtual, de los cuerpos, atribuyendo un papel cada vez más importante a las técnicas biométricas. Dibuja nuevas jerarquías y contribuye con fuerza a concentrar el poder.

En ella se encarna una pretensión de control total. Refleja una reducción de la acción política y social, que se limita al orden público, ya sin atención para las razones profundas de malestar o molestia, desigualdades o atropellos.

No es suficiente preguntarse si la privacidad puede sobrevivir en la edad del terror o, con paciencia, hacer una distinción entre distintas formas de vigilancia. Aunque los proyectos de vigilancia integral y global aún no sean realidad, el punto crítico es el paso entre una representación de la realidad y otra, afirmando que el «carácter excepcional» de ayer ya es «normal» hoy. La multitud ya no es «solitaria» y, por esta razón, sustraída también a la posibilidad de un continuo examen social. Ya está «desnuda», sin defensa frente a la pretensión pública o privada de un control general continuo.

En efecto, se afirma que no es posible utilizar el tradicional equilibrio entre distintos derechos cuando está en cuestión la supervivencia misma del Estado, como siempre en caso de guerras. Pero en el pasado la guerra se declaraba, existía un acto formal de comienzo y uno de conclusión: el «tiempo de guerra», con la posibilidad de limitar garantías constitucionales, tenía límites precisos. La guerra al terrorismo, por el contrario, no sólo no tiene limites, sino que además es intemporal: así definida por quien la conduce, es «una guerra infinita». ¿También la limitación de derechos y garantías será infinita? Además, la guerra contra el terrorismo es contra un enemigo invisible. ¿Esto puede significar que todos pueden transformarse posiblemente, si no en enemigos, por lo menos en sospechosos, legitimando todo tipo de control de masa? ¿Tenemos entonces que resignarnos a que el concepto mismo de libertad sea modificado?

Estas preguntas ni pueden ser eludidas ni pueden ser minimizadas. Se refieren a los caracteres mismos del sistema democrático, a las relaciones de legitimidad y proporción entre medios y fines. No es posible entonces utilizar astucias idiomáticas, representando esta importante cuestión como contraposición entre seguridad y privacidad, dejando entender que un importante interés común puede exigir el sacrificio de egoísmos o distinciones particulares. La apuesta no es, en efecto, una reducción limitada y menor en la esfera privada. Se discute sobre la dimensión de la libertad, y de esta manera la discusión se refiere a la relación entre seguridad y libertad, como han demostrado los análisis sobre las mutaciones acaecidas en Estados Unidos después del 11 de septiembre. Y la restricción de la libertad no constituye sólo un empobrecimiento «interior» de los sistemas democráticos, sino que debilita también la capacidad de acción hacia el «exterior» No debemos olvidar que uno de los objetivos de las acciones terroristas es también realizar una mutación de calidad de los regímenes democráticos, poniendo el acento sobre los aspectos autoritarios, y que las victorias de la democracia sobre los totalitarismos fueron posibles precisamente optando con fuerza y continuamente por un modelo basado en las libertades.

Creo que, desde esta perspectiva, es necesario profundizar en la relación entre democracia y tecnología. La tecnología es pródiga en promesas. Cada día ofrece más medidas para solucionar cualquier problema político, económico, social; sobre todo cuando se encuentran casos de tratamiento de datos personales. Y esta situación técnica determina una tentación permanente por los políticos de delegar en la tecnología la solución de problemas difíciles.

Hemos de discutir este planteamiento desde dos puntos de vista. El primero puede resumirse en la siguiente pregunta: ¿todo lo que es tecnológicamente posible es al mismo tempo éticamente admisible, socialmente aceptable, jurídicamente legítimo? Para contestar no creo que podamos aceptar la línea, que comienza con el pensamiento de HEIDEGGER, del carácter invencible del poder de la técnica como producción infinita de fines nuevos.

Ésta sería una conclusión inevitable si se acepta la deriva tecnológica en un desierto de valores democráticos. Por esto, frente al valor propio de la técnica, hoy mucho más que ayer necesitamos una reflexión continua sobre los valores básicos de la democracia, para distinguir entre los muchos usos de la tecnología democráticamente admisibles y los que no lo son.

De aquí se pasa al segundo punto de vista. Hay un gran riesgo para la política si confía totalmente en la tecnología: la reducción de todos los problemas a cuestiones de eficiencia o su transferencia a la sola dimensión del orden público.

Un ejemplo concreto. La videovigilancia se difunde, se presenta como la medida para solucionar muchísimos problemas de seguridad. Pero de esta manera los poderes públicos son incentivados a reducir el problema de una zona «de riesgo» a la sola lógica del orden público. De este modo se liberan de la obligación política de investigar las razones sociales y económicas que pueden estar en el origen de una situación de criminalidad y, por consiguiente, de proponer una estrategia más eficaz que la sola sanción penal.

En este contexto, la videovigilancia no hace más visible la sociedad: la oscurece. Esta utilización de la tecnología puede contribuir a establecer una política que rechaza los problemas difíciles, se aísla de la sociedad y cambia la naturaleza de la relación entre el ciudadano y el Estado. Y una política prisionera de la tecnología puede dar la impresión de mayor eficiencia, pero hace más débil la democracia.