SVRV Sachverständigenrat für Verbraucherfragen

Soberanía digital

Estudio científico del Consejo de Expertos en materia de Asuntos del Consumidor

Junio de 2017

Berlín, junio de 2017
ISSN 2510-0084

Editado por el

Consejo de Expertos en materia de Asuntos del Consumidor
en el Ministerio Federal Alemán de Justicia y Protección al Consumidor
Mohrenstraße 37
10117 Berlin

Teléfono: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525

Correo electrónico: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de
Esta publicación está disponible en internet.

Miembros del SVRV

[Consejo de Expertos en materia de Asuntos del Consumidor]

Prof. Dr. Lucia Reisch (presidente)
Profesora de Investigación intercultural del Consumo y Política europea del Consumidor en la Copenhagen Business School

Dr. Daniela Büchel (vicepresidente)
Miembro de la gerencia de REWE para los sectores de Recursos Humanos y Sostenibilidad

Prof. Dr. Gerd Gigerenzer
Director de la sección „Comportamiento adaptativo y Cognición“, así como del Centro Harding para Competencia en materia de Riesgo del Instituto Max-Planck para la Investigación de la Educación en Berlín

Helga Zander-Hayat
Directora del sector de Mercado y Derecho de la Organización de Consumidores de Renania del Norte-Westfalia

Prof. Dr. Gesche Joost
Profesora del área de Investigación en Diseño en la Universidad de Artes y Embajadora de Internet del Gobierno federal alemán en el gremio de los „Campeones Digitales“ de la UE

Prof. Dr. Hans-Wolfgang Micklitz
Profesor de Derecho económico en el Instituto Universitario Europeo de Florencia

Prof. Dr. Andreas Oehler
Profesor de Economía financiera en la Universidad de Bamberg y director de la sección de Investigación sobre Finanzas y Formación de los consumidores

Prof. Dr. Kirsten Schlegel-Matthies
Profesora de Economía doméstica en la Universidad de Paderborn

Prof. Dr. Gert G. Wagner
Profesor de Investigación económica empírica y Política económica en la Universidad Técnica de Berlín, miembro de la Presidencia del Instituto alemán de Investigación económica y Max Planck Fellow en el Instituto Max Planck para la Investigación en materia de Educación

Colaboradores del SVRV

Jefe del departamento:
Thomas Fischer, M.A.

Equipo científico del departamento:
Dr. Irina Domurath, Dr. Christian Groß

Estructura

Prefacio

Desde su constitución, el Consejo de Expertos en materia de Asuntos del Consumidor (SVRV) sigue trabajando en su tema principal „Consumidores en el mundo digital“ con diferentes priorizaciones. En su documento de política general „Política relativa al Consumidor en el mundo digital: Posición del Consejo de Expertos en materia de Asuntos del Consumidor“ (SVRV, 2015) el SVRV aboga por que la mayor cantidad de consumidores se beneficien de las ventajas de la digitalización mediante una concepción respetuosa de la protección de datos tecnológicos, a través del fortalecimiento de la competencia digital de los consumidores y mediante una regulación prudente. El SVRV no está solo en este tema: también en la política internacional del consumidor, como ha sido el caso en 2017 en el marco de las negociaciones de los ministros del G20 que tratan el tema digital, se trabaja en las condiciones marco para lograr una regulación orientada al bienestar común del mundo digital (Ministerio Federal Alemán de Economía (BMWi), 2017a).

Retomando estas demandas centrales, el presente estudio sigue la trayectoria de muchos trabajos anteriores del SVRV profundizando los aspectos tecnológicos de la digitalización en los sectores de la competencia de los consumidores y la regulación. El SVRV pone especial énfasis en el campo de la tecnología de fácil acceso para el consumidor mediante los estudios „El valor de los datos personales“[3] y „Tecnologías pro y contra la soberanía digital“[4]. Partiendo del documento „Mundo digital y Salud. Sanidad electrónica (eHealth) y Sanidad móvil (mHealth) – Oportunidades y Riesgos de la digitalización en el sector sanitario“ el SVRV reafirma la posición de que sin fortalecer la competencia digital se desperdician las oportunidades que ofrece la digitalización. El SVRV trató ya algunas cuestiones en materia de regulación en el estudio „Derechos del consumidor 2.0“, así como en el documento de trabajo „Precios personalizados“ en el que el SVRV hace referencia, por ejemplo, a requisitos del consentimiento, a la obligación de los oferentes de revelar información o el derecho a un acceso a ofertas sin discriminación.

3 Consultado el 20 de junio de 2017 en el URL http://www.svr-verbraucherfragen.de/wp-content/uploads/Open_Knowledge_Foundation_Studie.pdf.

4 Consultado el 20 de junio de 2017 en el URL http://www.svr-verbraucherfragen.de/wp-content/uploads/Weis_Lucks_Grassmuck_Studie_.pdf.

Un agradecimiento especial a Gesche Joost por la atención competente del estudio. En la preparación del estudio han trabajado también: Daniela Büchel, Gerd Gigerenzer, Hans Micklitz, Lucia A. Reisch, Kirsten Schlegel-Matthies, Gert G. Wagner y Helga Zander-Hayat.

El SVRV agradece a todos los colaboradores del SVRV por el amplio apoyo en la elaboración del estudio. Queremos agradecer especialmente al equipo científico del SVRV, Christian Groß, Irina Domurath y Mathias Bug.

Por lo demás, el SVRV agradece a los autores del estudio „Tecnología pro y contra la soberanía digital“, Rüdiger Weis, Stefan Lucks y Volker Grassmuck, así como a los autores del estudio „El valor de los datos personales: ¿Es el comercio de datos la mejor protección de datos?“, Walter Palmetshofer, Arne Semsrott y Anna Alberts, por haber aportado sus experiencias.

Para finalizar, cabe mencionar que la utilización de expresiones específicas de género en la formulación del presente texto se entenderá como aplicable tanto al género femenino como al masculino. Para garantizar una mejor legibilidad hemos renunciado a nombrar ambos géneros.

Berlín, junio de 2017

Por el Consejo de Expertos en materia de Asuntos del Consumidor

Lucia Reisch
Presidente del SVRV

Gesche Joost
Miembro del SVRV

Resumen

Al presentar el estudio „Soberanía digital“ el Consejo de Expertos en materia de Asuntos del Consumidor (SVRV) desea hacer un aporte al debate continuo sobre el desarrollo del concepto de la soberanía digital desde las perspectivas en materia de política para el consumidor.

Bajo el concepto de soberanía digital entendemos la capacidad de actuar y la libertad de decidir de los consumidores a la hora de desempeñar papeles diferentes en el mundo digital, es decir como operadores en el mercado, en calidad de ciudadanos consumidores de una sociedad, así como en carácter de „prosumidores“ en las redes. El concepto hace referencia, además, a los derechos y obligaciones de los ciudadanos en el marco normativo estatal y subraya las condiciones marco en las que un individuo puede utilizar medios y servicios digitales libremente, de forma competente y responsable y, de esa forma, estar en condiciones de participar activamente en calidad de ciudadano en una sociedad digital.

Nosotros identificamos cuatro directrices que están en relación con la soberanía digital: libertad de elección, autodeterminación, autocontrol y seguridad. Para poder hacer realidad estas directrices proponemos las siguientes medidas que deberían adoptarse en los campos de acción de la tecnología de fácil acceso para el consumidor, la competencia digital y la regulación.

Tecnología

- **Crear un portal de datos centrado en el consumidor:** el SVRV recomienda el desarrollo de un portal de datos centrado en el consumidor (tablero de mandos) para materializar la soberanía individual de datos.

- **Introducir principios de privacidad desde el diseño y de privacidad por defecto:** el SVRV reafirma la exigencia de una configuración predefinida de los sistemas de comunicación (privacidad / seguridad desde el diseño y privacidad / seguridad por defecto como directrices) que sea accesible para el usuario, consuma menos datos y, al mismo tiempo, esté orientada a la seguridad. Los proyectos fomentados de forma estatal deberán regirse por estas directrices.

- **Aumentar la seguridad en el internet de las cosas:** de cara a los problemas de seguridad cada vez más graves en el segmento del internet de las cosas, el SVRV recomienda verificar cómo se puede garantizar que, a imagen de los procedimientos en el sector sanitario, se puedan asegurar de forma continua y comprometida los productos y servicios puestos en circulación a través del ciclo vital completo por medio de actualizaciones de seguridad. Será necesario desarrollar estándares tecnológicos y depositar de forma duradera códigos fuente (de forma análoga a la „fórmula“ utilizada en el sector alimenticio).

- **Ampliar la oferta de productos que consuman menos datos:** el SVRV recomienda verificar si se puede conceder a los consumidores un derecho a la utilización de productos digitales que recopilen menos datos y que les permita tener la posibilidad de poder escoger una variante digital que recoja menos datos.

Competencia digital

- **Cerrar un pacto de cualificación para la „competencia digital en la formación de docentes“:** el SVRV recomienda realizar un pacto de cualificación para la „competencia digital en la formación de docentes“ (de forma análoga al pacto de calidad de la enseñanza o a la ofensiva de calidad en la formación de docentes).

- **Apoyar las ofertas para fomentar la competencia digital:** el SVRV recomienda financiar de forma permanente y afianzar estructuralmente las ofertas ya existentes para fomentar la competencia digital o las (institucionales) que puedan establecerse en el futuro. Para lograrlo se deberán ampliar sistemáticamente las ofertas que sirvan de hilo conductor, las ofertas para multiplicadores y las ofertas para los consumidores.

- **Desarrollar medidas de autocontrol al utilizar medios y servicios digitales:** el SVRV recomienda a los ministerios de cultura desarrollar medidas para fomentar el autocontrol al utilizar los medios y servicios digitales.

- **Estudiar los efectos de la digitalización en la cognición, la emoción y la vida social:** el SVRV recomienda el fomento específico de la investigación interdisciplinaria sobre los efectos de la digitalización en la cognición, la emoción y la vida social de los consumidores. Esto afecta tanto a los „aborígenes digitales", como así también a los „migrantes digitales".

Regulación

- **Formular CGC (Condiciones Generales de Contratación) y declaraciones en materia de protección de datos de forma breve en una sola página (one-pager):** el SVRV reafirma la recomendación de que antes de concluir un contrato las empresas informen al consumidor en una sola página (500 palabras) sobre las normas relevantes respecto al derecho en materia de protección de datos, así como las disposiciones de las CGC. El SVRV recomienda que esa idea de „una sola página" se implemente por medio de un proyecto piloto organizado por el Ministerio Federal Alemán de Justicia y Protección al Consumidor (BMJV) con sectores interesados importantes.

- **Revelar algoritmos y permitir que sean verificables:** el SVRV reafirma la recomendación de asegurar mediante normas legales (a) que los algoritmos tengan en cuenta las normas de los derechos del consumidor, del derecho en materia de protección de datos, del derecho en materia de antidiscriminación y de la seguridad digital, así como hacer transparentes los parámetros en los que se basan los algoritmos que estén en contacto directo con los consumidores y (b) que mediante la obligación estandarizada de revelar informaciones se revelen estos algoritmos a un círculo de expertos que mediante la toma de pruebas al azar verifique la seguridad legal. El SVRV recomienda desarrollar estándares legales y depositar de forma duradera los códigos fuente.

- **Mejorar el derecho a la información gratuita:** el Consejo de Expertos recomienda garantizar el derecho a la información gratuita (artículo 34 de la BDSG [Ley Alemana sobre Protección de Datos]) sin limitaciones, así como obligar a las empresas a informar a los consumidores de forma transparente, entendible y fácilmente reconocible sobre el derecho que los consumidores tienen a la información y a la posibilidad de rectificar datos erróneos al ofrecer sus productos (es decir rectificación, eliminación y bloqueo).

- **Seguir desarrollando estándares mínimos para la interoperabilidad:** el SVRV recomienda desarrollar estándares mínimos que garanticen una cierta compatibilidad entre los servicios digitales de forma tal que sea posible una comunicación entre las cuentas de usuario independientemente de los oferentes (interoperabilidad – de forma análoga a la telefonía móvil).

- **Concretizar el derecho a la portabilidad de los datos:** el SVRV reafirma la recomendación de entender el derecho a la portabilidad de los datos como el derecho a rescisión de contrato y recomienda fijar un marco para poder cambiar entre los diversos oferentes (de forma análoga a las transacciones de pago digital).

1. Estado del debate

Hoy en día, los productos y servicios digitales penetran en la vida cotidiana de los consumidores y plantean nuevos desafíos para la política del consumidor. Los dispositivos terminales móviles aptos para internet tienen cada vez más difusión y son utilizados especialmente por adolescentes, casi todos los entrevistados de 12 a 19 años los utilizan (Feierabend et al., 2016). También si se toma la población total de Alemania, las cifras de usuarios son altas y, actualmente, alcanzan los dos tercios de la población (Initiative D21, 2016). Incluso de las personas denominadas „silver surfers" (es decir usuarios mayores de 60 años) aproximadamente la mitad de los menores de 70 años navega regularmente en la red y un cuarto de los mayores de 70 años (Initiative D21, 2016; Destatis, 2016).

Al mismo tiempo, se puede apreciar una crisis creciente de confiabilidad por parte de los consumidores frente a los prestadores de servicios en línea en lo que se refiere a la utilización (palabras clave: comercio de datos y grandes datos) y seguridad de sus datos (palabras clave: ataques de piratas informáticos e incidentes de phishing), así como la veracidad de los contenidos en línea (palabra clave: desinformación selectiva y/o „falsas noticias"). Según un estudio de Orange (2014) casi el 80 por ciento de los consumidores desconfía de los prestadores de servicios en línea y considera que la utilización de datos no es transparente. Sin embargo, la mayoría de los usuarios sigue estando dispuesta a dar sus datos personales si a cambio puede utilizar los servicios (sobre la utilización de datos con fines publicitarios véase Destatis, 2016). Esto provoca una relación de poder asimétrica entre las empresas y los individuos: las primeras tienen acceso a los datos individuales, mientras que los consumidores no lo saben y no tienen control al respecto (World Economic Forum, 2014).

Utilización de datos: Una razón posible de la crisis de confiabilidad descrita es la creciente cantidad de servicios en línea cuyo modelo comercial se basa en la recopilación y valoración de una gran cantidad de datos (véase, por ejemplo, Christl & Spiekermann, 2016; Karaboga et al., 2014; sobre la difusión de la utilización en Alemania: Destatis, 2016). Esto conduce a una „huella digital" que permite obtener una imagen detallada del comportamiento individual del consumidor, su entorno social y sus preferencias (Golder & Macy, 2014) posibilitando así un pronóstico mediante grandes datos. Como consecuencia, de los datos se pueden obtener por ejemplo informaciones sobre el comportamiento de pago y/o la predisposición de pago de los consumidores y, por lo tanto, crear precios personalizados (Schleusener & Hosell, 2015; Zander-Hayat et al., 2016a; Zander-Hayat et al., 2016b). Esta evolución hace que plataformas en línea como Google, Facebook, Amazon y YouTube tengan una especial importancia dado que estas empresas han logrado un poder de mercado considerable en el segmento en línea y, frecuentemente, faltan ofertas alternativas desde el punto de vista de los consumidores o no son lo suficientemente atractivas. También forma parte de la realidad la presión de grupo que sienten muchos consumidores que los obliga a conectarse y consumir a través de las plataformas mencionadas. A pesar de que, en principio, desde el punto de vista técnico es posible cambiar el oferente, esto casi no se hace dado que la interoperabilidad entre los oferentes presenta muchas lagunas y, por consiguiente, la portabilidad de los datos de usuario hacia el nuevo oferente es muy complicada y no justamente sencilla para el usuario.

Seguridad de datos: además, desde el punto de vista de los consumidores es necesario actuar en el mercado en línea para crear una arquitectura eficaz en materia de seguridad. Esto queda probado mediante la creciente cantidad de experiencias personales con la criminalidad en línea, como la difusión de virus informáticos, la usurpación de identidad y el abuso de los datos de la banca en línea (Birkel et al., 2014; Rieckmann & Kraus, 2015; Bug et al., 2015; Oficina Federal de Investigación Criminal, 2016). Además, la confianza de los consumidores en la seguridad de sus dispositivos terminales se ha visto perturbada, entre otras cosas, mediante los últimos ataques de denegación de servicio[3] en partes del internet de las cosas – „Objetos cotidianos inteligentes" que están conectados con internet (Möchel, 2016; Weis et al., 2016).

Contenidos en línea: Además, en las redes sociales y en las páginas web motivadas ideológicamente se pro-

3 En el caso de un ataque (distribuido) de denegación de servicio se envían muchas consultas realizadas al mismo tiempo desde diferentes aparatos a uno o varios servidores hasta que éstos estén sobrecargados. Tales ataques no son ocasionales. Proveedores de servidores y empresas especializadas los pueden interceptar en parte. Pero esto se vuelve más difícil cuanto los ataques son más fuertes y de mayor duración (Kühl & Breitegger, 2016).

paga el fenómeno de la desinformación selectiva (palabra clave: „falsas noticias"; véase, por ejemplo, Kucharski, 2016; Spinney, 2017) que demanda una gran capacidad de valoración por parte de los usuarios a la hora de evaluar la credibilidad de las fuentes y los contenidos. Por lo demás, prácticamente uno de cada de cinco jóvenes alemanes ya ha tenido experiencias personales con acoso o mobbing en línea y difamación en los medios sociales. A este resultado arribó un estudio de YouGov realizado en el año 2015 por orden de Vodafone.[4] Aproximadamente un tercio de los entrevistados indicaba que algún amigo o miembro de su familia ya había sido acosado alguna vez en internet. En general, a causa de este tipo de incidentes o similares se ha reducido considerablemente la sensación de seguridad en estos espacios semipúblicos.

Por lo tanto, era de esperar que la recuperación y el fortalecimiento de la confianza de los consumidores en todas estas dimensiones estuviera a en el centro de la política digital del consumidor. Pero la mejor forma de lograr y fortalecer la confianza legítima en el mundo digital es que los consumidores puedan actuar de forma soberana en el mundo digital. Entretanto, la discusión en materia de política del consumidor sobre la soberanía digital en Alemania lleva ya, por lo menos, diez años y se remonta a la „Carta sobre la soberanía del consumidor en el mundo digital" (BMELV [Ministerio Federal Alemán de Alimentación, Agricultura y Protección del Consumidor], 2007) que fue presentada en ocasión del Día Mundial de los Derechos del Consumidor en 2007 bajo la impresión del aumento veloz de todas las formas de relaciones comerciales digitales. Los autores utilizan por primera vez el concepto de „Soberanía del consumidor" en el contexto digital y definen las directrices de un diseño del mundo digital favorable para el consumidor. Además, se hace referencia al derecho fundamental de „autodeterminación informativa".

Sobre la base del estudio del BMELV, en el debate en materia de política para el consumidor se desarrollaron paso a paso las acciones recomendadas para el fortalecimiento de la soberanía digital. El informe en materia de política para el consumidor presentado por el Gobierno federal alemán en el año 2008 retoma el mensaje principal de la Carta y designa la competencia de los consumidores como requisito básico para tomar decisiones responsables en el mundo digital (Gobierno federal, 2008). También la „ Agenda Digital 2014 - 2017" del Gobierno federal alemán considera que especialmente el fortalecimiento de la competencia medial de los consumidores es una medida central para proteger al consumidor en el mundo digital, junto con los observadores del mercado, el derecho de acción colectiva, así como ajustes iniciales que protejan la esfera privada ante las aplicaciones digitales (privacidad desde el diseño y privacidad por defecto) (Gobierno federal, 2014). El BMWi [Ministerio Federal Alemán de Economía y Energía] tiene una opinión similar y considera que la adquisición de competencias clave, seguridad informática y protección de datos son las condiciones para la soberanía digital (BMWi, 2015). Junto con los aspectos del aseguramiento de la identidad, así como la protección ante la usurpación de identidad, el Gobierno federal alemán indica en el Informe en materia de política para el consumidor del año 2016 que „el fortalecimiento de la autodeterminación, la garantía de libertad de elección y de transparencia, informaciones amplias y entendibles para el consumidor y la seguridad en la red" son los objetivos de la política del consumidor (Gobierno federal, 2016).

En el presente estudio retomamos esta idea de soberanía digital (individual) y la separamos de la soberanía digital nacional[5]. Consideramos que el concepto de la soberanía de datos[6], que constituye un concepto central en el debate en materia de política para el consumidor, es un aporte importante en materia de soberanía digital para nuestro concepto en el sentido de libertad de elección de los consumidores

4 Consultado el 14 de junio de 2017 en el URL http://docs.dpaq.de/9635-ppt_for_vodafone cyberbullying_-_germany_060_9_9_15.pdf.

5 El concepto de soberanía digital se ha utilizado, especialmente, en el curso del debate sobre las revelaciones de Edward Snowden, muchas veces también relacionado con una soberanía nacional de la infraestructura digital (Friedrichsen & Bisa, 2016). Después de que se dieran a conocer las actividades de observación masivas llevadas a cabo, especialmente, por los servicios secretos estadounidenses se empezó a exigir una soberanía digital de los estados europeos y sus ciudadanos, por ejemplo, mediante una infraestructura digital independiente o a través del fortalecimiento de las competencias nacionales de producción de hardware (BMWi, 2015). También Bitkom, la Asociación Federal Alemana para la Tecnología de la Información, subraya el aspecto nacional de soberanía digital (Bitkom, 2015): en consecuencia, la soberanía digital apunta a la „independencia de algunos espacios económicos, estados y empresas al adquirir y utilizar tecnologías digitales y fabricar plataformas". Bitkom describe la soberanía digital más como anexo a esa caracterización económica, como elemento que también los consumidores (junto con empresas y administraciones) pueden emplear en „tecnologías y soluciones digitales de forma segura, autónoma y autodeterminada".

6 Heiko Maas (Maas, 2015) indica que el consentimiento para recopilar, tratar, etc. datos personales es la clave de la soberanía de datos y lamenta que al ser tan largas las CGC el consentimiento tenga tan sólo una función de excusa y, por lo tanto, sólo sea una simulación de autodeterminación. Según sus propias declaraciones el „Libro verde de las plataformas digitales" basado en un proceso de diálogo con la economía, la ciencia y la sociedad recupera el concepto de „soberanía de datos" como declaración de principios sin dar explicaciones en detalle y/o realizar una limitación del

sobre la recopilación, el tratamiento y la utilización de sus datos personales. Son los consumidores quienes tienen que tomar la decisión de si, por ejemplo, desean donar sus datos personales con fines de beneficencia, si los quieren vender o si prefieren impedir su recopilación. Siguiendo esta idea, soberanía digital y ahorro de datos son antípodas como, en parte, ya se suponía (por ejemplo, BMWi, 2015). Por el contrario, tendría que ser posible que el ahorro de datos fuera una manifestación de soberanía digital autodeterminada por los consumidores.

En consecuencia, entendemos como soberanía digital la capacidad de acción y la libertad de decisión de los consumidores de poder actuar en el mundo digital en roles diferentes, tanto como operador en el mercado o en calidad de ciudadano consumidor de una sociedad, así como „prosumidor" en las redes. El concepto hace referencia, además, a los derechos y obligaciones de los ciudadanos en el marco estatal del orden y subraya las condiciones marco bajo las cuales los ciudadanos pueden utilizar los medios y servicios digitales de forma libre, competente y responsable y, por lo tanto, estar en condiciones de participar activamente en una sociedad digital. Inspirándonos en el debate sobre la soberanía del consumidor en el mundo digital (BMELV, 2007; Gobierno federal, 2016), así como en el análisis de Mertz et al. (2016) identificamos cuatro directrices que están en relación con la soberanía digital: *libertad de elección, autodeterminación, autocontrol* y *seguridad*. Nosotros proponemos que se implementen mediante *tecnología* de fácil acceso para el consumidor, *competencia digital* de los consumidores, así como *regulación*.

Con el presente estudio el SVRV quiere hacer una contribución al debate para el desarrollo del concepto de la soberanía digital desde las perspectivas en materia de política para el consumidor. Basándonos en este posicionamiento recomendamos acciones concretas para cuya implementación se deberá contactar a diferentes actores. El estudio está desarrollado de la siguiente forma: en el capítulo 2 deducimos cuatro directrices de la soberanía digital (libertad de elección, autodeterminación, autocontrol y seguridad) y argumentamos que la soberanía digital se debería fomentar mediante tecnología, competencia digital y regulación favorable para el consumidor („triángulo de la soberanía digital"). En los capítulos 3 a 5 presentamos para los tres campos de acción esbozos breves específicos sobre el problema complementados con acciones recomendadas en materia de política para el consumidor.

concepto de soberanía digital. Sin embargo, el estudio tiene también un componente referido a la política del consumidor: se subraya que es muy importante asegurar que los consumidores tengan un trato soberano de sus datos, incluyendo el poder disponer de quien pueda estar en posesión de esos datos (BMWi, 2016). El „Libro blanco de las plataformas digitales del BMWi" discute sobre soberanía de datos en el marco del Reglamento de base en materia de protección de datos de forma paralela al aspecto de la portabilidad de los datos, sin ahondar en los conceptos que se esconden detrás (BMWi, 2017b). La „Carta de Derechos Digitales Fundamentales de la Unión Europea" (consultado el 14 de junio en el URL https://digitalcharta.eu/) habla de „soberanía de datos" e indicando que se trata, por ejemplo, del derecho a disponer de los datos propios o también del requisito del consentimiento para la recopilación y la utilización de datos personales. Se menciona el desafía que la digitalización implica para la enseñanza: la formación digital como tal, pero entendida como el derecho a poder vivir en el mundo digital de forma autodeterminada.

2. Concepto: directrices y campos de acción

2.1. Cuatro directrices: libertad de elección, autodeterminación, autocontrol y seguridad

En cuanto a la clasificación del concepto de la soberanía digital nos orientamos al concepto de soberanía del consumidor (por ejemplo, Hutt, 1940; Persky, 1993; Schwarzkopf, 2011). El concepto abarca tanto un nivel empírico descriptivo („Cuán soberanos son los consumidores?“ y/o „Qué determinantes se interrelacionan con la soberanía del consumidor?“) así como también un nivel prescriptivo normativo („Cuán soberanos tendrían que ser los consumidores?“ y/o „Qué medidas se deberían tomar para poner a los consumidores en condiciones de actuar de forma soberana?“) y describe en qué posición se encuentran demandantes y oferentes en el mercado y/o en qué posición tendrían que estar (Schwarzkopf, 2011).

Mertz et al. (2016) siguen un planteamiento empírico descriptivo en el artículo „Autodeterminación digital“. Aquí se describe qué aspectos están en relación con la autodeterminación digital (aquí: competencia, información, valores, posibilidad de elección, voluntariedad, generación de voluntad, actuación) y qué factores determinan fundamentalmente la autodeterminación digital (aquí: determinantes técnicas, socioculturales y personales). Aquí la soberanía digital está definida como el „despliegue concreto de una personalidad humana y/o la posibilidad de realización de los propios proyectos y decisiones de accionar en tanto esto afecte a un empleo consciente de los medios digitales o sea (co)dependiente de la existencia o modo de funcionamiento de los medios digitales“ (Mertz et al., 2016). Los autores presentan, además, numerosas paralelas entre el concepto de la autodeterminación digital y el concepto de la autodeterminación informativa (Mertz et al., 2016).

En el presente estudio continuamos el debate en el nivel prescriptivo normativo y analizamos qué condiciones marco concretas se deben crear para que los consumidores sean capaces de actuar de forma autodeterminada en un mundo que está cada vez más conectado digitalmente (véase también Rau, 2016).

Siguiendo el estudio de Mertz et al. (2016), así como el discurso en materia de política para el consumidor sobre la soberanía del consumidor en el mundo digital (BMELV, 2007; Gobierno federal, 2016) identificamos cuatro directrices que están en relación con la soberanía digital: *libertad de elección, autodeterminación, autocontrol* y *seguridad*.

Libertad de elección se entiende en sentido amplio y abarca tanto los aspectos de la libertad de acción negativa („liberarse de algo“) como así también de la libertad de acción positiva („ser libre de hacer algo“). Por consiguiente, los consumidores deberían ser lo suficientemente libres para hacer algo o no hacerlo (Mertz et al., 2016). Traspasado al contexto del consumidor en el mundo digital esto puede significar, por ejemplo, que al comprar una aplicación los usuarios tienen, fundamentalmente, la opción de escoger entre una variante gratuita (divulgando sus datos de usuario) o variante pagada (sin divulgar sus datos de usuario) según cual sea su preferencia (Weis et al., 2016). La libertad de elección también puede expresarse en que los consumidores en el caso de un cambio de oferente no tengan considerables inconvenientes para la transacción. Así se evitan los efectos de cautividad que puedan generarse a causa de la falta de portabilidad de datos – ocasionada a través de „silos de información“ y falta de estándares para posibilitar una verdadera interoperabilidad (BMWi & BMJV, 2015). Los consumidores poseen libertad de elección especialmente también cuando se transforman en „administradores activos“ de sus propios datos: entonces pueden decidir de forma autónoma sobre transmisión, retiro, eliminación, donación y comercialización de sus datos – siempre y cuando no existan otros intereses importantes para otros actores que estén legalmente fundados (por ejemplo, Palmetshofer et al., 2016). También forma parte de la libertad de elección la decisión de si se debe permitir que otros tengan acceso a los datos personales.

Autodeterminación en el trato con medios digitales significa que los usuarios de hardware y software tienen la soberanía sobre las decisiones importantes. De esto se deduce que los consumidores no deben ser el objeto de decisiones automatizadas sobre la base de algoritmos que son de considerable importancia para el estilo de vida de los consumidores. Por ejemplo, si el procedimiento de calificación utilizado para decidir sobre el otorgamiento de un crédito a un consu-

midor está completamente automatizado y carece de transparencia esto puede ocasionar considerables problemas si la base de datos y la lógica del algoritmo utilizado no se dan a conocer, porque en ese caso falta la base para el derecho a oposición. Esta evolución se vuelve más explosiva cuanto más amplios sean los métodos de calificación empleados al relacionar diferentes tipos de datos (Weis et al., 2016). Por lo tanto, la imputación a fines específicos en el caso de la recopilación y utilización de datos personales es un factor de importancia al igual que la opción de guardar y analizar los datos de forma anonimizada. El principio de la autodeterminación implica también que los consumidores puedan estimar el riesgo de manipulación (Mertz et al., 2016) que se genera, por ejemplo, mediante el empleo de social bots[7], así como a través de la propagación de desinformación selectiva (las denominadas „falsas noticias"). Junto con medidas tecnológicas y normativas apropiadas son imprescindibles también una formación digital básica y la alfabetización de los datos.

Autocontrol significa que los usuarios estén en condiciones de conocer los límites de la propia utilización de ofertas digitales y medir las consecuencias de su comportamiento. Teniendo en cuenta los cientos de aplicaciones disponibles, el internet de las cosas y la posibilidad de estar permanentemente en línea cobra cada vez más importancia el hecho de que las personas mantengan el control sobre su estilo de vida y no sean manejados por el mundo digital o incluso dependientes de él. Autocontrol significa también no distraerse con el móvil o correos electrónicos entrantes cuando se conduce y desconcentrarse (Helbing et al., 2017). Además de los posibles trastornos de concentración se han documentado casos de dependencia de medios digitales, llamada también „adicción a internet".[8] Esa dependencia de los medios digitales lleva a algunas personas a un alto grado de estrés tecnológico (Gigerenzer, 2010). Nuestra idea de soberanía digital abarca, por lo tanto, no solamente la concepción de una actuación soberana dentro del mundo digital, sino que exige un trato igualmente soberano del mundo digital en el sentido de tener la capacidad de poder controlar los servicios digitales o dispositivos terminales como el teléfono inteligente (smartphone) cuando se los utiliza y no ser controlados o influenciados por ellos de forma decisiva.

Seguridad significa garantizar la protección de los datos del consumidor y de las infraestructuras digitales a través del Estado y las empresas, así como a través de los consumidores mismos. Para ello deben estar disponibles las infraestructuras que permitan una recopilación y un almacenamiento seguros, así como una transmisión controlada de datos. La gran cantidad de ataques cibernéticos a ordenadores privados, como también los casos de robo de carteras de clientes a empresas internacionales son una prueba de la gran importancia para la política del consumidor. Las configuraciones técnicas predefinidas como privacidad desde el diseño y privacidad por defecto pueden facilitarles a los consumidores una vida cotidiana segura en el mundo digital y, al mismo tiempo, confortable. A su vez, la disponibilidad de tecnologías de encriptado de fácil uso como también actualizaciones regulares de seguridad son elementos importantes para la seguridad de los consumidores en la red. Conocimientos básicos de los factores centrales de la seguridad en la red es la tarea de una formación educativa para todos los grupos de edades e instituciones.

2.2. Tres campos de acción: tecnología, competencia digital y regulación

Sobre la base de los trabajos anteriores del SVRV descritos antes, proponemos lograr las directrices de soberanía digital indicadas mediante *tecnología de fácil acceso para el consumidor, competencia digital*, así como la constitución de un marco a través de regulación del mundo digital en el sentido del bienestar común. Podemos describir la soberanía digital desde tres perspectivas: primero, como cuestión de condiciones marco tecnológicas para servicios y productos que requieren muchos datos, segundo, como cuestión de la educación para enseñar las capacidades y habilidades necesarias para tratar informaciones, fuentes y datos en línea y tercero, como cuestión de regulación de la utilización de datos personales y como fortalecimiento de los derechos del consumidor. Estos tres campos de acción en conjunto conforman el triángulo de la soberanía digital.

7 Social bots son programas de computación que están en condiciones de responder de forma automática en los medios sociales (Ferrara et al., 2016).

8 „Internet addiction is typically described as a state where an individual has lost control of the internet use and keeps using internet excessively to the point where he/she experiences problematic outcomes that negatively affects his/her life"(Young & Abreu, 2011; cf. Kardefelt-Winther, 2014).

Como tecnología entendemos aquí especialmente „facilitadores“ tecnológicos, es decir aquellas funciones, principios y aplicaciones que posibilitan un comportamiento digital soberano o lo impiden cuando faltan. Aquí se trata, por ejemplo, de gestión de datos, actualizaciones de seguridad o utilización de tecnologías de encriptado y principios del ahorro de datos orientados al usuario.

La competencia digital abarca aspectos como el tratamiento de informaciones y de una posible desinformación selectiva („falsas noticias“), la utilización de medios de comunicación digitales y de herramientas digitales, la capacidad de gestionar datos, así como la posesión de conocimientos sobre productos y conceptos relacionada con esto y la predisposición a aprender de forma autónoma toda la vida. El fortalecimiento de la competencia digital pone a los consumidores además en condiciones de utilizar medios digitales de forma autocontrolada que va desde la utilización moderada hasta la no utilización autodeterminada.

La regulación abarca tanto los derechos y obligaciones de cada consumidor, así como los derechos y obligaciones de las empresas y el Estado. Los derechos y obligaciones de cada consumidor se refieren, por ejemplo, al derecho a la eliminación y a la portabilidad de los datos, así como la obligación de instalar actualizaciones de seguridad en los aparatos del internet de las cosas. Los derechos y obligaciones de las empresas y del Estado se refieren especialmente a la transparencia y a la asignación a fines específicos a la hora de recopilar y utilizar datos, así como la verificabilidad y la revelación de algoritmos, por ejemplo, en el marco de auditorías de algoritmos, como ya se practica hoy en el sector de calificación crediticia.

Imagen 1: Triángulo de la soberanía digital:
tecnología, competencia digital y regulación (representación propia)

El modelo está concebido para describir las relaciones causales entre los campos de acción indicados para la política del consumidor. De esto se deduce que es importante avanzar en los tres campos de acción para posibilitar la soberanía digital de los consumidores. Aquellos consumidores que son conscientes del valor de sus datos y desean imponer sus derechos en la red no pueden, por ejemplo, actuar de forma soberana si las condiciones marco tecnológicas se lo impiden o si no pueden trasladar sus datos a otros prestadores de servicios o si no tienen ninguna posibilidad de elección al utilizar sus datos. Al mismo tiempo, una regulación de los mercados de datos solamente puede ser eficaz si se realiza la implementación tecnológica y los consumidores pueden hacer uso de sus derechos. Por lo tanto, para complementar el modelo de autodeterminación digital de Mertz et al. (2016) subrayamos, especialmente, la interrelación y el fortalecimiento recíproco (o también debilitamiento) de los factores individuales que constituyen la soberanía digital.

De forma similar al concepto presentado aquí, De Mooy (2017) identifica tres campos de acción interrelacionados que tienen como objetivo una soberanía individual de datos. De Mooy identifica en su estudio educación, portabilidad de los datos, autorregulación de las empresas y una verificación regulada por el Estado en calidad de precursora hacia una mayor soberanía de datos. Sin embargo, en el concepto presentado aquí el objetivo del concepto de la soberanía digital es más amplio. Por lo tanto, los campos de acción han sido ampliados.

Según nuestra opinión, la soberanía digital resulta siempre de un equilibrio entre tecnología, competencia digital y regulación, sin darle prioridad a ninguno de los tres factores y sabiendo que los tres componentes pueden estar dirigidos tanto a las autoridades y la economía como así también al individuo mismo. A continuación, presentaremos nuestras recomendaciones en los tres campos de acción para el fortalecimiento de la soberanía digital de los consumidores.

Tecnología

3. Tecnología

En lo sucesivo se discutirán aspectos técnicos centrales de importancia para la soberanía digital de los consumidores. Aquí se trata, especialmente, de la protección y utilización de datos, así como de los aspectos de seguridad que tienen importancia creciente dado que el mundo está cada vez más conectado.

3.1. Crear un portal de datos centrado en el consumidor

El SVRV recomienda el desarrollo de un portal de datos centrado en el consumidor (tablero de mandos) para materializar la soberanía individual de datos.

El SVRV recomienda el desarrollo de un portal de datos centrado en el consumidor (tablero de mandos) para materializar la soberanía individual de datos. Allí los consumidores tendrán transparencia para la utilización (alcance, contenido) de sus datos individuales a través de diferentes oferentes en la red y los podrá eliminar o modificar de forma centralizada y administrar los derechos de acceso.

El acceso a un tablero de mandos tal deberá estar asegurado a través de un derecho individual que se pueda imponer. Ese portal de datos podría implementarse de forma práctica, por ejemplo, mediante una iniciativa conjunta del Estado y las empresas.

Para el desarrollo de un portal de datos centrado en el consumidor, se encuentran en primer plano la transparencia para el tratamiento de datos, descentralización en el mercado de datos y el empleo de estándares técnicos como por ejemplo MyData[9] (véase también Jentzsch, 2017). MyData formula los siguientes derechos para una interfaz de todos los datos personales y/o personalizados almacenados a los que tuviera acceso el consumidor individual: el derecho a saber qué informaciones personales existen a ver el contenido real de los datos personales a corregir datos incorrectos a verificar quien tiene acceso a los datos personales y porqué, a recibir datos personales y utilizarlos libremente, a compartir informaciones personales con terceros o venderlas, eliminar datos personales, etc. (Palmetshofer, Semsrott & Alberts, 2016). La denominada Gestión de las Relaciones con los vendedores (VRM, por sus siglas en inglés), así como la plataforma Hub-of-All-Things (HAT) [Centro de todas las cosas] tienen planteamientos similares (Palmetshofer et al., 2016).

Cabe recordar que la idea principal en el caso de la creación de un portal de datos centrado en el consumidor es la conducción descrita del flujo de datos a través de consumidores. Por el contrario, en el caso del desarrollo del portal de datos la posibilidad de comercializar los datos propios no tendría que ser el tema principal, sino solamente un escenario posible para los consumidores. De cara a la comercialización de los datos propios el SVRV ha constatado que, actualmente, la monetización de datos prácticamente no es realizable para los consumidores y, probablemente, sólo podrían beneficiarse del comercio de datos los consumidores que dispongan de la alfabetización necesaria de los datos (Data Literacy). Tampoco han sido discutidos de forma suficiente los aspectos éticos en el caso del comercio en línea con datos personales, como por ejemplo datos físicos. Además, cabe recordar que, actualmente, para los consumidores es muy difícil establecer un precio justo para sus propios datos (SVRV, 2016). En la mayoría de los casos, al utilizar servicios en línea los consumidores aceptan una relación comercial sin poder estimar la plusvalía que sería posible sobre la base de los datos generados o transmitidos. Los factores que influyen la sensibilidad de los consumidores de cara a de la utilización de sus datos son, por un lado, variables fácilmente medibles como tipo de datos, prestadores de servicios, dispositivo utilizado o forma de recopilar y utilizar datos, por otro lado, variables subjetivas como la confianza en el prestador de servicios y el beneficio real o imaginario resultante para los consumidores (World Economic Forum, 2014). También los factores culturales son importantes. Por ejemplo, los consumidores en los países escandinavos y bálticos parecen ser menos sensibles en materia de datos que los alemanes.

Para la investigación es, actualmente, casi imposible desarrollar ensayos, modelos y estándares para deter-

9 Consultado el 14 de junio de 2017 en el URL http://mydata.org.

minar el valor de los datos individuales (Palmetshofer et al., 2016; Jentzsch, 2016). Sin embargo, comienza a notarse que, en el caso de los modelos de utilización actuales, el cálculo del precio posible y/o del valor económico de los datos es, presumiblemente, demasiado bajo (Palmetshofer et al., 2016). Además, se plantea el interrogante de la recuperabilidad de los datos y con ello la pertenencia real de los datos. A esto se suma el problema de que, frecuentemente, muchos datos empiezan a ser valiosos gracias a su reproducción, sin embargo, los grandes archivos de datos generados apenas pueden remitirse a los respectivos consumidores individuales. Los consumidores no siempre poseen posibilidades u opciones técnicas o la autorización de descargar sus datos personales del respectivo servicio utilizado. Aun cuando esto fuera posible, en la mayoría de los casos reprocesar o reconectar los datos con otros exige conocimientos avanzados de computación.

Otro planteamiento para un control del flujo de datos más accesible para el consumidor es la implementación de un sistema de recomendación conocedor del contexto (World Economic Forum, 2014). Un sistema tal podría ser el mediador entre el prestador de servicios que solicita la utilización de datos y el consumidor mismo. Sobre la base de diversos factores como la historia del usuario, la configuración básica, el tipo de utilización de datos, etc., el sistema de recomendación le sugeriría o desaconsejaría al consumidor la utilización de la prestación de servicios si, por ejemplo, tuviera reparos en materia de protección de datos. Además, el sistema podría estar desarrollado con capacidad de autoaprendizaje de forma tal que aprenda a través de las decisiones del consumidor. Tales datos sobre sistemas pueden apoyar al consumidor cuando éste tome una decisión sobre la idoneidad de las condiciones comerciales y los modelos de plusvalía sobre la base de datos individuales y aumentar la utilidad. Sin embargo, este planteamiento se encuentra hasta ahora tan sólo en la fase conceptual de forma tal que, en este momento, podemos recomendar tanto el portal de datos centrado en el consumidor como así también el sistema de recomendación como proyectos de desarrollo futuro para la soberanía digital de los consumidores.

3.2. Introducir principios de privacidad desde el diseño y de privacidad por defecto

El SVRV reafirma la exigencia de una configuración predefinida de los sistemas de comunicación (privacidad / seguridad desde el diseño y privacidad / seguridad por defecto como directrices) que sea accesible para el usuario, consuma menos datos y, al mismo tiempo, esté orientada a la seguridad. Los proyectos fomentados de forma estatal deberán regirse por estas directrices.

La directriz privacidad desde el diseño significa que la confidencialidad es un elemento natural en la concepción y estructuración de sistemas de comunicación para proteger la esfera privada de los consumidores. La directriz privacidad por defecto significa que la configuración básica garantiza en gran medida la esfera privada y la protección de datos y, partiendo desde esa configuración básica, los consumidores tienen la posibilidad de cambiar fácilmente a un modo de comunicación que consuma menos datos.

Lo mismo vale para los principios de seguridad desde el diseño y seguridad por defecto en lo que se refiere a la seguridad de la comunicación y los servicios utilizados. Al respecto, es necesario que todos los usuarios, especialmente aquellos que no disponen de una profunda capacidad informativa y digital, estén en condiciones de proteger sus datos de forma sencilla y efectiva, así como de poder comunicarse con seguridad.

El logro de la confidencialidad (es decir „privacidad“) en la comunicación y la transmisión de los datos del consumidor siguen teniendo un papel principal para el SVRV (véase Reisch et al. 2015, SVRV, 2015). Al respecto, es para nosotros muy importante que también aquellas personas que no disponen de una profunda capacidad informativa puedan proteger sus datos de forma sencilla.[10] Esta idea se ve respaldada mediante la directiva en materia de privacidad y comunicaciones electrónicas del año 2002 que sigue teniendo va-

10 Domurath & Kosyra (2016) ofrecen un panorama sobre las denominadas tecnologías de protección de la intimidad.

lidez. En el considerando 46 se consideran necesarias medidas como

> "obligar a los fabricantes de determinados tipos de equipos utilizados en los servicios de comunicaciones electrónicas a que fabriquen sus productos de manera que incorporen salvaguardias para garantizar la protección de los datos personales y la intimidad del usuario y del abonado." (Directiva en materia de privacidad y comunicaciones electrónicas 2002/58/CE)

Además, la demanda se orienta a los conceptos enunciados en el Reglamento de base en materia de protección de datos de la UE (artículo 25 I, II):

> „exige la adopción de las oportunas medidas de carácter técnico y organizativo con el fin de garantizar el cumplimiento de lo dispuesto en la presente Directiva. La aplicación de tales medidas no puede depender únicamente de criterios económicos. A fin de poder demostrar que cumple lo dispuesto en la presente Directiva, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que respeten, en particular, los principios de la protección de datos desde la concepción y de la protección de datos por defecto." (Reglamento de base en materia de protección de datos de la UE, considerando 78)

Privacidad y/o seguridad desde el diseño significa que confidencialidad y otras características de seguridad son elementos naturales de los sistemas de comunicación en el sentido de que las correspondientes funcionalidades se vean implementadas o sean desarrolladas en el sistema de comunicación para lograr la confidencialidad (Weis et al., 2016; Domurath & Kosyra, 2016). El principio de privacidad desde el diseño indica que los datos deberían ser tratados fundamentalmente de forma local allí donde está el consumidor y/o que los datos solamente sean transmitidos de forma anonimizada, seudoanonimizada (o agregada), así como encriptada y autenticada (Weis et al., 2016).

Privacidad y/o seguridad por defecto describe la posibilidad de elección que tienen los consumidores para cambiar fácilmente de un modo de comunicación menos seguro a uno más seguro, sin embargo, predeterminado („por defecto") es siempre el modo seguro. Por lo tanto, privacidad y/o seguridad por defecto sólo puede entenderse como una configuración predefinida que asegura que los datos personales estén automáticamente protegidos en sistemas informáticos o modelos comerciales sin que la persona afectada tenga que tomar medidas para proteger su esfera privada (Domurath & Kosyra, 2016).[11]

3.3. Aumentar la seguridad en el internet de las cosas

De cara a los problemas de seguridad en el segmento del internet de las cosas que son cada vez más graves, el SVRV recomienda verificar cómo se puede garantizar que, a imagen de los procedimientos en el sector sanitario, se puedan garantizar de forma continua y comprometida los productos y servicios puestos en circulación a través del ciclo vital completo por medio de actualizaciones de seguridad. Será necesario desarrollar estándares tecnológicos y depositar de forma duradera códigos fuente (de forma análoga a la „fórmula" utilizada en el sector alimenticio).

La protección en el segmento del internet de las cosas tendría que ser una obligación para el fabricante al momento de escribir actualizaciones de seguridad. Además, existe la posibilidad de verificar de qué forma se puede depositar el código fuente de un sistema por ejemplo en manos de un fideicomisario si el fabricante no cumple su obligación de desarrollar actualizaciones de seguridad. En ese caso también habría que verificar la posibilidad de hacer público el texto fuente (fuente abierta). Esto permitiría asegurar que, por lo menos, terceras personas puedan ocuparse de escribir y, dado el caso, divulgar las actualizaciones de seguridad.

11 De la privacidad por defecto se debe separar la privacidad por opción: aquí los consumidores pueden cambiar entre modos más o menos seguros, sin que la configuración predefinida sea necesariamente el modo más seguro (Weis et al., 2016).

En el sentido de la seguridad de los consumidores en el mundo digital, la industria informática ha desarrollado y mejorado permanentemente una gestión de seguridad para clientes particulares y empresas apoyada por actualizaciones regulares y en parte automáticas de software, así como a través de ciclos de actualización de hardware relativamente cortos. Si bien, a pesar de todos los esfuerzos, algunos productos de software ampliamente difundidos como Adobe Flash, así como Microsoft Windows y Office vuelven a estar siempre en la mira de los investigadores de la seguridad que critican los puntos débiles en la arquitectura de la seguridad (BSI [Oficina Federal Alemana para la Seguridad en la Técnica de la Información], 2016), hay que constatar que la seguridad en los relativamente nuevos aparatos del internet de las cosas es claramente peor que antes (Weis et al., 2016).

Esto se puede explicar dado que en el internet de las cosas se venden y utilizan, frecuentemente, aparatos de bajo precio con una fidelización de clientes mínima (por ejemplo, bombillas aptas para internet o cámaras IP) y, a causa del corto ciclo de producción, muchas veces, las empresas no se sienten responsables de informar a los consumidores sobre las actualizaciones de seguridad necesarias (Weis et al., 2016). Sin embargo, también existen graves problemas de seguridad en aparatos del internet de las cosas con una vida relativamente larga, como por ejemplo sistemas de calefacción inteligentes, dado que exigen muchos años de mantenimiento del hardware y del software incluido, cosa que probablemente ningún oferente esté en condiciones de realizar. Además, muchas veces los consumidores carecen de los conocimientos necesarios para realizar el mantenimiento del hardware y, mucho menos, del software de tales aparatos (Weis et al., 2016). En este caso se le exige a la industria estándares de fácil acceso para el consumidor que garanticen en la vida diaria la implementación de una infraestructura segura en el internet de las cosas.

Considerando las muchas señales que hablan de una cierta inseguridad en el segmento del internet de las cosas, nosotros abogamos por la toma de medidas más efectivas para garantizar la seguridad en el internet de las cosas. De ellas forma parte la obligación del fabricante de escribir actualizaciones de seguridad.

Además, existe la posibilidad de verificar de qué forma se puede depositar el código fuente de un sistema por ejemplo en manos de un fideicomisario si el fabricante no cumple su obligación de desarrollar actualizaciones de seguridad. En ese caso también habría que verificar la posibilidad de hacer público el texto fuente (fuente abierta). Esto permitiría asegurar que, por lo menos, terceras personas puedan ocuparse de escribir y, dado el caso, divulgar las actualizaciones de seguridad. Si el fabricante no cumple las obligaciones indicadas o si el fabricante ya no existe, el fideicomisario se encargará de la publicación de los textos fuente en calidad de fuente abierta.

3.4. Ampliar la oferta de productos que consuman menos datos

El SVRV recomienda verificar si se puede conceder a los consumidores un derecho a la utilización de productos digitales que recopilen menos datos y que les permita tener la posibilidad de poder escoger una variante digital que recoja menos datos.

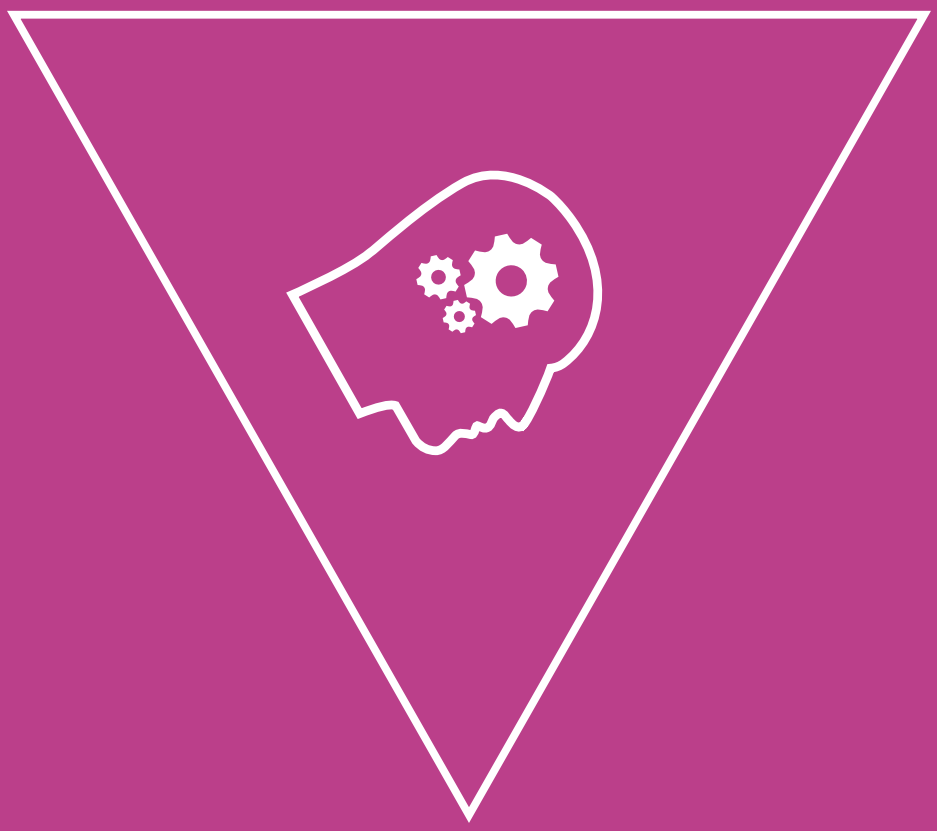
Los usuarios deben poder decidir si, al utilizar servicios y productos digitales, desean dar informaciones sobre la propia utilización de los medios o hacerlo sólo en parte o renunciar por completo sin que se vean restringidas las funciones básicas de un producto digital. Los consumidores que no deseen dar ningún dato no deberán verse perjudicados (de forma análoga al derecho en materia de antidiscriminación). Esto implica para las transacciones comerciales que no puede tener consecuencias negativas si una consumidora decide, por ejemplo, adquirir productos y servicios en línea sin abrir una cuenta de cliente o divulgar sus datos de otra forma (dado que no son directamente necesarios para el procesamiento del contrato).

Una característica importante de la soberanía digital es la elección de la representación de los contenidos digitales, por ejemplo, en páginas de internet. Esto abarca la posibilidad de poder utilizar los

denominados bloqueadores de publicidad sin que la utilidad de la página de internet se vea limitada.[12] A pesar de que somos conscientes de que las ofertas (exclusivamente) financiadas mediante publicidad han perdido cifras de ventas a causa del aumento del empleo de bloqueadores de publicidad, en el sentido de la libertad de elección de la presentación de ofertas en línea estamos en contra de la prohibición de bloqueadores de publicidad. En su propio interés, la industria publicitaria tendría que darse cuenta de que la aparición de publicidad en gran formato, probablemente incluso personalizada y, frecuentemente, como ventana emergente (formato pop-up) o con volumen sumamente alto que no se puede desconectar y exige un volumen de datos enorme y puede ser interpretada como una molestia considerable y una limitación de la experiencia del usuario. Si las informaciones deseadas en una página de noticias en internet con contenidos periodísticos solamente ocupan una pequeña parte del contenido emitido, entonces se trata de una desproporción que debe ser solucionada en el sentido del consumidor. Habría que dedicarle más atención al aspecto de la molestia previsible ocasionada por la publicidad, así como al aspecto de la rastreabilidad de los intereses personales a través de la publicidad ofrecida.

Además, en esos casos habría que aplicar el derecho en materia de antidiscriminación para que un individuo pueda decidir si quiere dar a conocer sus datos (digitales). Esto implica para las transacciones comerciales, que no puede tener consecuencias negativas si un consumidor decide, por ejemplo, adquirir productos y servicios en línea sin abrir una cuenta de cliente o divulgar sus datos de otra forma, en tanto esto sea posible (Becker, 2017).

12 Bloqueadores de publicidad son extensiones para el navegador que modifican los contenidos publicitarios modificando de forma apropiada para los usuarios los contenidos de páginas web con el objetivo de lograr una representación sin publicidad, así como limitar las informaciones sobre la utilización de los medios que será transmitida a los oferentes de páginas web (véase al respecto también Ofiera, 2016).



Competencia digital

4. Competencia digital

La digitalización modifica de forma decisiva la forma de producir, poner a disposición y difundir informaciones en una sociedad. Para poder utilizar de forma soberana y autodeterminada las nuevas posibilidades y oportunidades de la sociedad digital se les exige también a los consumidores que tengan nuevas competencias. La libertad de elección, la autodeterminación, el autocontrol y la seguridad en la red exigen que se tenga competencia digital.

Información y alfabetización en el uso de datos [data literacy] describen conjuntamente lo que se ha dado en llamar alfabetización digital [digital literacy], una nueva técnica cultural junto con la lectura, la escritura y la calculación. Los consumidores deben estar en condiciones de determinar cuál es su necesidad de informaciones, encontrar, estimar y valorar informaciones de cara a su importancia, calidad, alcance y pertinencia, tratar y reprocesar informaciones y, dado el caso, también posibilitar el acceso a otros (por ejemplo, Süss, 2017). Estas competencias son importantes, independientemente de si las informaciones son análogas o digitales.

Sin embargo, realmente han aparecido determinados fenómenos en el contexto de los medios digitales que son importantes para la utilización y evaluación digital competente de las informaciones almacenadas. Como, por ejemplo, la (no)eliminabilidad de datos, la diferenciación entre contenido redaccional, formatos publicitarios clásicos y contenidos generados por los usuarios (incluyendo el márketing influyente en plataformas como YouTube e Instagram), así como contenidos generados automáticamente mediante robots sociales [social bots] (al respecto, por ejemplo, Wineburg et al., 2016). Además, tienen implicaciones para la protección de datos y el derecho de autor en el trato con informaciones puestas en la red representando así un nuevo problema. Esta rápida evolución tecnológica exige que el desarrollo de las competencias de los usuarios también sea rápido.

A continuación, se formularán objetivos centrales para fomentar la competencia digital de los consumidores. Estos abarcan la cualificación necesaria de docentes, así como la ampliación de la oferta de informaciones confiables sobre el consumidor. Además, vemos la necesidad de actuar en el sector del autocontrol digital, así como también la necesidad de investigación con vistas a los efectos de la digitalización en la cognición, emoción y la vida social. Al mismo tiempo, se presentan interrogantes éticos en relación con el comercio de datos, la pérdida de control en el internet de las cosas o la libertad de elección de los consumidores, que también contienen las respectivas dimensiones jurídicas. De ello resulta la necesidad de investigación interdisciplinaria para la política del consumidor que debe ser cubierta a través del fomento específico.

4.1. Cerrar un pacto de cualificación para la „competencia digital en la formación de docentes“

El SVRV recomienda realizar un pacto de cualificación para la „competencia digital en la formación de docentes“ (de forma análoga al pacto de calidad de la enseñanza o a la ofensiva de calidad en la formación de docentes).

El establecimiento de un paquete de medidas sustentado conjuntamente por el gobierno nacional y los estados federados para la „competencia digital en la formación de docentes“ deberá contribuir a garantizar el establecimiento de la competencia digital en la primera y segunda fase de la formación de docentes, así como a asegurar en el futuro el perfeccionamiento y la capacitación para los requerimientos permanentemente cambiantes en el mundo digital. El enfoque principal debe estar puesto sobre todo en las discusiones fructíferas sobre la digitalización y no en la digitalización de la clase o del equipamiento técnico.

Junto con las competencias en el trato con medios y herramientas digitales, así como para la aplicación de formas y métodos de enseñanza digitales (incluso exámenes) habrá que tratar también en la formación, el perfeccionamiento y la capacitación de los docentes actuales y futuros cuáles son sus competencias en el trato con las oportunidades y consecuencias individuales y sociales de la digitalización. La libertad de elección, la autodeterminación, el autocontrol y la seguridad en lo que se refiere a la digitalización en todos los ámbitos de vida (con medios digitales, pero también con el internet

de las cosas, etc.) exigen competencias que deben ser adquiridas mediante diferentes medidas de formación.

Si no se tiene en cuenta de forma correspondiente en la formación de docentes, serán incompletas las iniciativas como la estrategia „Educación en el mundo digital“ (Conferencia Permanente de los Ministros de Educación y Asuntos Culturales, 2016) en la que los estados federados de Alemania han acordado un marco de competencia para la formación digital. Por un lado, esto va dirigido a las disciplinas técnicas, las metodologías didácticas y las ciencias de la educación en los centros de altos estudios que forman docentes. Por otro lado, esto afecta la segunda fase de la formación de docentes, es decir la época de las prácticas, así como las instituciones de perfeccionamiento y capacitación para enseñantes que deben elaborar conceptos integrales para la creación sucesiva de competencia digital en la formación de docentes. Por consiguiente, los „Requisitos de contenido comunes a los estados federados para las disciplinas técnicas y las metodologías didácticas en la formación de docentes“ (Conferencia Permanente de los Ministros de Educación y Asuntos Culturales, 2008; cf. 2017[13]) deberán ser adaptados para lograr competencias digitales también en los estándares obligatorios de las asignaturas destinadas a formar docentes.

4.2. Apoyar las ofertas para fomentar la competencia digital

El SVRV recomienda financiar de forma permanente y afianzar estructuralmente las ofertas que ya existan o las (institucionales) que puedan establecerse para fomentar la competencia digital. Para lograrlo se deberán ampliar sistemáticamente las ofertas que sirvan de guía, las ofertas para multiplicadores y las ofertas para los consumidores.

Las ofertas (institucionales) para fomentar la competencia digital para multiplicadores y consumidores pueden contribuir a la ampliación de la competencia porque pueden facilitar informaciones confiables y probadas, funcionar como hilo conductor y reaccionar de forma rápida a la evolución en el mundo digital.

Guías como, por ejemplo, la Fundación Warentest (fundación alemana para la evaluación de productos), ponen a disposición de los consumidores informaciones confiables sobre productos y servicios entre otros en los sectores de inversión, educación y productos para el hogar. De esta forma, los consumidores se ven en condiciones de tomar decisiones de consumo libremente sin informaciones aportadas por los sectores interesados. Por ejemplo, en el sector sanitario existe el problema de que los consumidores no pueden diferenciar las informaciones confiables de aquellas aportadas por interesados. En este caso, el Instituto de Calidad y Rentabilidad en el Sector sanitario (IQWiG) podría asumir tal función de guía elaborando una lista positiva de fuentes basadas en evidencias y entendibles, que se actualice y difunda regularmente.

Una oferta que sirve de guía para multiplicadores es, por ejemplo, la orientación sobre materiales [Materialkompass] para la Formación de los consumidores, mientras que la „Guía de capacitación“ de la Fundación Warentest y el „Banco de datos sobre competencia medial“ del Organismo alemán de Educación Política se dirigen directamente a los consumidores. Además, habría que captar otras iniciativas y asociaciones como, por ejemplo, la Initiative D21 y el Chaos Computer Club, como actores adicionales para recoger la evolución de la digitalización y poder implementarla en ofertas de información, esclarecimiento y formación.

El fomento de la competencia digital fuera de la escuela y otras instituciones educativas desempeña un papel central de cara al veloz desarrollo de las aplicaciones digitales y las costumbres cambiantes de los usuarios. Para reducir la complejidad los consumidores precisan un acceso rápido a informaciones confiables y relevantes en todos los sectores de consumo (véase al respecto también Gigerenzer et al., 2016). Ofertas que sirvan de guía brindando informaciones verificadas y esenciales pueden ser de gran ayuda. Por esta razón, el SVRV propone que, por ejemplo, de forma análoga a la función de la Fundación Warentest (fundación alemana para la evaluación de productos) o del IQWiG[14], se establezcan y promocionen ofertas que sirvan de guía para los consu-

13 Consultado el 14 de junio de 2017 en el URL https://www.kmk.org/themen/allgemeinbildende-schulen/lehrkraefte/lehrerbildung.html.

14 Consultado el 14 de junio de 2017 en el URL https://www.iqwig.de/.

midores en diferentes campos de consumo. En „Mobilsicher.de“,[15] un portal de internet para fomentar la seguridad de la comunicación móvil a través del teléfono inteligente y tabletas de la asociación iRights e.V., así como en Marktwächer.de[16], Checked4u.de[17] y Verbraucherzentrale.de[18], en los que organizaciones de consumidores procesan entre otras cosas informaciones sobre ofertas digitales como portales de evaluación, plataformas y servicios de “yo cuantificado” se ponen a disposición informaciones confiables para el consumidor.

Tales Ofertas que sirven de guía son también una ayuda para multiplicadores en diferentes sectores. Un ejemplo es la orientación sobre materiales [Materialkompass] de Formación de los consumidores; evalúa materiales didácticos sobre asuntos del consumidor entre otros en el sector de los medios (sobre temas como protección de datos, conocimientos básicos y derecho, así como violencia en la red) y sirven de gran ayuda tanto para asegurar la calidad de los materiales didácticos como así también a los docentes para estructurar la clase. El SVRV propone una consolidación de la oferta para proporcionar a los docentes una orientación al elegir materiales didácticos de mayor calidad en el sector de la formación digital. Una orientación tal es sumamente importante porque los materiales didácticos ofrecidos por asociaciones, editoriales, organizaciones no gubernamentales y el sector público, así como por empresas se utilizan cada vez más en clase, pero no están sometidos a ninguna verificación.[19]

Junto con actividades que tienen como objetivo el fomento de la competencia digital en el contexto escolar se deben ampliar y financiar ofertas de formación que promuevan la competencia digital en el contexto extraescolar. Un ejemplo es la „Weiterbildungs-Guide“ [Guía de capacitación] de la Fundación Warentest (fundación alemana para la evaluación de productos)[20] o el Banco de datos sobre competencia medial del Organismo alemán de Educación Política[21]. En el banco de datos se encuentra una lista de proyectos de pedagogía mediática que tienen como objetivo el fomento de la competencia medial. Allí se puede buscar por tipo de medios o por oferta.

15 Consultado el 14 de junio de 2017 en el URL https://mobilsicher.de/.
16 Consultado el 18 de junio de 2017 en el URL www.marktwaechter.de.
17 Consultado el 18 de junio de 2017 en el URL www.checked4u.de.
18 Consultado el 18 de junio de 2017 en el URL www.verbaucherzentrale.de.
19 Consultado el 14 de junio de 2017 en el URL http://www.verbraucherbildung.de/artikel/lehrkraefte-wollen-unabhaengige-qualitaetstests-von-unterrichtsmaterial.
20 Consultado el 14 de junio de 2017 en el URL http://weiterbildungsguide.test.de/.
21 Consultado el 14 de junio en el URL http://www.bpb.de/lernen/digitale-bildung/medienpaedagogik/206263/medienkompetenz-datenbank.

Otras ofertas de gran ayuda son Digitalkompass.de,[22] un proyecto combinado para fomentar la competencia medial de personas mayores, así como „Watch your Web“[23] (finalizado en el año 2015), un portal de información que ofrece informaciones y formación mediática para jóvenes orientada a la protección del consumidor en las redes sociales.

4.3. Desarrollar medidas de autocontrol al utilizar medios y servicios digitales

El SVRV recomienda a los ministerios de cultura desarrollar medidas para fomentar el autocontrol al utilizar medios y servicios digitales.

El control propio en lugar del ajeno al utilizar medios y servicios digitales es un elemento esencial de la competencia digital. Esto abarca la capacidad de controlar servicios digitales y/o dispositivos terminales como móviles en lugar de ser controlado por ellos. Los efectos de la falta de control se hacen cada vez más visibles, por ejemplo, a través de la creciente cantidad de accidentes de tránsito mortales por utilizar el móvil al conducir. Dado que tales formas de comportamiento se desarrollan muy pronto es necesario comenzar a tomar medidas para fomentar el autocontrol digital ya en la edad preescolar.

En el año 2016, la Conferencia Permanente de los Ministros de Educación y Asuntos Culturales se dedicó al tema „Educación en el mundo digital“. Al mismo tiempo, su estrategia común a todas las instituciones educativas y disciplinas puede aplicarse a escolares/estudiantes y docentes. En ese planteamiento se ha dejado de lado la gran importancia que tiene al utilizar tecnologías digitales poseer el control digital propio en lugar de estar sometido al ajeno. El autocontrol es un elemento esencial de la competencia digital. Esto implica la capacidad de controlar servicios digitales o dispositivos terminales como el teléfono inteligente cuando se los quiere utilizar según las propias preferencias, pero también el comportamiento individual en foros y en las redes sociales, así como el cumplimiento de las reglas del buen com-

22 Consultado el 14 de junio de 2017 en el URL https://www.digital-kompass.de/.
23 Consultado el 14 de junio de 2017 en el URL http://www.watchyourweb.de/.

portamiento en la red (sin incitación al odio ni acoso cibernético, etc.; Underwood & Ehrenreich, 2017).

Los efectos de la falta de control se hacen cada vez más visibles, por ejemplo, a través de la creciente cantidad de accidentes de tránsito mortales por utilizar el internet al conducir. Pero también cabe mencionar la distracción que provocan los correos electrónicos entrantes y los respectivos trastornos de concentración. Una encuesta representativa de Bitkom Research arrojó como resultado que ya el 51 por ciento de los conductores lee noticias breves mientras conduce y el ocho por ciento mira videos en su teléfono inteligente.[24] La National Highway Traffic Safety Administration (2015) informa que uno de cada siete accidentes documentados en los EE.UU. estaba relacionado con la distracción del conductor por utilizar el móvil.

La creciente necesidad de utilizar servicios digitales mientras se realizan otras actividades (multifuncionalidad) puede llevar a una reducción de la capacidad cognitiva de control como, por ejemplo, la reducción del abanico de atención y de la capacidad de permanecer concentrado en una tarea en la vida cotidiana, mientras que la hipótesis de una adaptación exitosa a la multifuncionalidad es controvertida (Ophir et al., 2009; van der Schuur et al., 2015). La utilización paralela de servicios digitales y redes sociales durante los seminarios tiene un efecto negativo sobre el rendimiento académico y los resultados de los exámenes (Ellis et al., 2010; Junco, 2012; Rosen et al., 2011; Wood et al., 2012). Ya en el año 2012 el 69 por ciento de los estudiantes estadounidenses confesaba que escribía mensajes durante los seminarios, el 28 por ciento usaba Facebook y el 21 por ciento buscaba contenidos ajenos al tema que se estaba tratando (Junco, 2012) y entre el 49 y el 70 por ciento utilizaba Facebook mientras hacía sus tareas (Junco, 2015). La falta de autocontrol digital puede desembocar en dependencia, llamada también „adicción a internet“ (Helbing et al., 2017; Young & Abreu, 2011; véase Kardefelt-Winther, 2014).

Para reducir estas consecuencias negativas de las tecnologías digitales, es necesario desarrollar el autocontrol como elemento esencial para ser competente en el mundo digital. Este autocontrol digital tendría que desarrollarse ya en la edad preescolar y también los padres tendrían que dar el ejemplo (Gigerenzer, 2017). Sin embargo, hasta ahora casi no existe ninguna investigación sobre métodos eficaces de autocontrol en el mundo digital de forma tal que el SVRV considera que aquí es especialmente necesaria la investigación para poder aclarar (1) qué intervenciones ayudan a las personas a formar el autocontrol digital, (2) cómo se pueden integrar estas intervenciones ya en la edad (pre)escolar y (3) qué medios técnicos y legales pueden ser un apoyo para compensar la falta de autocontrol.

24 Consultado el 14 de junio en el URL https://www.bitkom.org/Presse/Presseinformation/Viele-Autofahrer-nutzen-waehrend-der-Fahrt-das-Smartphone.html.

4.4. Estudiar los efectos de la digitalización en la cognición, la emoción y la vida social

El SVRV recomienda el fomento específico de la investigación interdisciplinaria sobre los efectos de la digitalización en la cognición, la emoción y la vida social de los consumidores. Esto afecta tanto a los „aborígenes digitales“ como así también a los „migrantes digitales“.

Actualmente, se analiza la competencia digital poniendo especial énfasis en el trato con la técnica. Por el contrario, se investiga de forma insuficiente en qué medida se modifican las formas de comportamiento psíquico y social y qué consecuencias traerá aparejado esto. Desde hace años se especula sobre posibles transformaciones sistemáticas de la atención, de los sentimientos y del comportamiento social de las personas a través de la digitalización, pero falta la investigación sistemática, especialmente sobre los efectos a largo plazo de los medios sociales.

Al mismo tiempo, se presentan los interrogantes éticos en relación con el comercio de datos, la pérdida de control en el internet de las cosas o la libertad de elección de los consumidores y sus respectivas dimensiones jurídicas. En este caso, se presenta una necesidad de investigación interdisciplinaria para la política del consumidor que solamente puede ser cubierta a través del fomento específico.

Teniendo en cuenta el entusiasmo de niños y adolescentes por los medios digitales es sorprendente que la investigación del desarrollo psicológico se haya ocupado hasta ahora muy poco de sus repercusiones sobre el des-

arrollo y el comportamiento (Underwood & Ehrenreich, 2017). ¿Qué impacto tiene sobre el desarrollo la interacción con los adultos que se ha visto sumamente deteriorada a causa del consumo digital (véase Barr, 2010)? ¿Qué consecuencias tiene una captación superficial de información („Shallow Learning“) para la capacidad de pensar de forma independiente y la consolidación de contenidos (Loh & Kanai, 2016)? ¿Es un problema el reducido abanico de atención que poseen muchas personas que se ve reforzado por la multifuncionalidad o se puede aprender también a obtener el mismo rendimiento con permanentes interrupciones? ¿Qué relaciones y colaboraciones se establecen entre el ser humano y la máquina y cuáles son sus consecuencias? Se desconocen las respuestas a estas y otras preguntas importantes.

Junto con los efectos de la revolución digital sobre las capacidades cognitivas se puede suponer también que la vida social y emocional ha cambiado claramente. Se habla mucho de casos de acoso cibernético y, realmente, se lastima a muchos jóvenes por internet, pero frecuentemente, de forma diferente a la que suponen los adultos. Los jóvenes padecen de exclusión social cuando ven imágenes de sus amigos que se han encontrado sin decir nada o fotos de fiestas a las que no han sido invitados (Underwood & Ehrenreich, 2017). La disponibilidad digital permanente no solamente se espera en los medios sociales, sino también en la vida profesional, y se discute como factor de estrés social (Carstensen, 2015). La no utilización de medios digitales por un corto tiempo, de forma voluntaria o no, también se siente frecuentemente como una situación de gran estrés, semejante al caso de adicción. La delegada del Gobierno federal alemán para planes de drogas parte actualmente de aproximadamente 600.000 adictos a internet y 2,5 millones de usuarios problemáticos de internet en Alemania (Fundación Kind und Jugend, 2017). El uso intenso del teléfono móvil y el ordenador son factores de riesgo para trastornos del sueño asociados a consecuencias para la salud (por ejemplo, Thomée, 2012; van der Schuur et al., 2015). Por lo demás, la utilización del teléfono inteligente pone en peligro los efectos positivos de la interacción social real (Rotondi et al., 2017). Además, hay señales de una vinculación entre la utilización intensa de los medios por parte de los padres y trastornos en el desarrollo de los hijos, por ejemplo, trastornos en la adquisición del lenguaje e hiperactividad motriz en el caso de los niños menores de seis años (Fundación Kind und Jugend, 2017).

Sin embargo, también se puede observar una evolución positiva. Se puede constatar un fuerte crecimiento del alcance de las comunidades en línea que fortalece el compromiso civil (por ejemplo, Better Place, Code for Germany, Next Hamburg) y posibilita nuevas formas de participación. También el interés político encuentra formas complementarias en la red (véase al respecto, por ejemplo, el proyecto MAZI financiado por la UE[25]) y fomenta las comunidades.

También para muchos es una gran ayuda en la vida cotidiana tener la posibilidad de un intercambio en foros específicos sobre temas personales sensibles (por ejemplo, grupos de autoayuda en línea) que pueden ser utilizados de forma anónima (por ejemplo, Döring, 2010). Las relaciones diversas entre el ser humano y el sistema interconectado también aparecen cada vez más intensamente en el centro de atención del entorno laboral si los trabajadores pueden ser apoyados en tiempo real a través de aplicaciones de realidad aumentada[26] y, por lo tanto, se abren nuevos campos de acción o si el acceso a los conocimientos en la fuente abierta de ecología puede desplazar las posibilidades de producción y a largo plazo potencialmente también las relaciones de poder (véase Rifkin, 2014). Se trata de investigar los interrogantes éticos, jurídicos y sociales que resulten a largo plazo.

Para entender mejor de qué forma la tecnología digital nos modifica a todos y cómo podemos controlar las consecuencias negativas y, al mismo tiempo, comprender y apoyar la evolución positiva es imprescindible estudiar de forma sistemática los efectos de la revolución digital sobre las personas. La cuestión central para la investigación no debe ser si los medios digitales influyen sobre el desarrollo cognitivo, sino de qué forma modifica la tecnología a los usuarios y qué competencias necesitan los usuarios para poder hacerle frente de mejor manera (Gigerenzer, 2013; 2017). La investigación tendría, sobre todo, que aclarar (1) qué efectos tiene la utilización de servicios digitales sobre el desarrollo infantil y juvenil y qué intervenciones favorecen un comportamiento sano (2), qué impacto tiene sobre los „migrantes digitales y (3) qué condiciones marco institucionales y legales se deben crear para que tanto los „aborígenes digitales“ como así también los „migrantes digitales“ puedan manejar y controlar mejor los efectos psíquicos, sociales, económicos y de salud de la revolución digital.

25 Consultado el 14 de junio de 2017 en el URL http://www.mazizone.eu/.
26 Véase al respecto por ejemplo, el proyecto smartFactory de Predictive Maintenance Data Analysis (consultado el 14 de junio de 2017 en el URL http://dfki-3036.dfki.de/webNews/SF_Steckbrief_20151118_LabsNetworkIndustrie.pdf).

Regulación

5. Regulación

La lógica de actuación de la regulación tiene como objetivo exigir de los actores estatales y de la economía privada que asuman su responsabilidad para garantizar la soberanía digital. En cuanto a la dimensión legal, el concepto de la soberanía digital de los consumidores se ve reflejado en el derecho a la autodeterminación informativa protegido constitucionalmente conforme al artículo 2 apartado 1 página 1 de la GG [Ley Fundamental Alemana].[27] El derecho a la autodeterminación informativa se vio concretizado en la sentencia sobre el censo nacional del BVerfG [Tribunal Constitucional Federal de Alemania] basada en el artículo 2 apartado 1 y 1 apartado 1 de la GG. Este abarca fundamentalmente el derecho de cada persona a „autodeterminar sobre la divulgación y utilización de sus datos personales". Desde entonces se considera la autodeterminación informativa como la condición previa necesaria de la libertad real, tanto en relación con el Estado como así también en relación con los actores privados (Buchner, 2006). El ámbito de protección del derecho general a la privacidad abarca también la posibilidad de obtener un panorama de las partes esenciales de la vida de una persona o una idea concluyente de su personalidad mediante un acceso al sistema.[28]

A la responsabilidad estatal por la garantía de autodeterminación informativa de los ciudadanos sigue la obligación de recibir y, dado el caso, mejorar las condiciones marco jurídicas para el ejercicio de la autodeterminación informativa. Es de suma importancia que el Estado sirva de ejemplo dado que también las normas excepcionales para medidas en el sector de la seguridad interna deben atenerse de forma estricta al marco legal, posibilitando la transparencia de la actuación estatal y el cumplimiento de los límites definidos por los tribunales superiores[29].

En ese sentido, en lo sucesivo se detallan algunas acciones recomendadas para sectores concretos en los que el SVRV considera que es imprescindible una actuación reguladora.

5.1. Realizar CGC (Condiciones Generales de Contratación) y declaraciones en materia de protección de datos de forma breve en una sola página (one-pager)

El SVRV reafirma la recomendación[30] de que antes de concluir un contrato las empresas informen al consumidor en una sola página (500 palabras) sobre las normas relevantes respecto al derecho en materia de protección de datos, así como sobre las disposiciones de las CGC. El SVRV recomienda que esa idea de „una sola página" se implemente por medio de un proyecto piloto organizado por el Ministerio Federal Alemán de Justicia y Protección al Consumidor (BMJV) con sectores interesados relevantes.

La obligación de „una sola página" puede contribuir a aumentar la transparencia para los consumidores en la transmisión de datos. Además, „una sola página" puede contribuir a elevar la aceptación de las CGC y las declaraciones en materia de protección de datos utilizadas si esta página se redacta conjuntamente en un proceso de cooperación entre el BMJV u otra autoridad estatal y sectores interesados.

El consentimiento de las personas afectadas en tal recopilación de datos es un pilar de la autodeterminación informativa y, por lo tanto, de la soberanía digital de los consumidores. En la práctica, el consentimiento se realiza mediante declaraciones estandarizadas en materia de protección de datos. Sin embargo, la concientización sobre la recopilación y el tratamiento de los datos y los correspondientes derechos del

27 Crítica al concepto de la autodeterminación informativa: Friedewaldt et al. (2017).

28 BVerfG [Tribunal Constitucional Federal de Alemania], sentencia del 27.02.2008 - 1 referencia 370/07 - BVerfGE [Recopilación de sentencias del Tribunal Constitucional Federal de Alemania] 120, 274, 314 (Registros en línea).

29 Especial importancia tienen las decisiones sobre el almacenamiento de datos digitales de comunicación de toda la sociedad ordenado por el Estado. Para Alemania al respecto: BVerfG sentencia del 2.3.2010, 1 referencia 256; TJCE, sentencia del 21 de diciembre de 2016 en los asuntos judiciales relacionados C-203/15, Tele2 Sverige AB / Post- och telestyrelsen y C-698/15, Secretary of State for the Home Department / Tom Watson entre otros, ECLI:EU:C:2016:970; TJCE, sentencia del 8. April 2014 en los asuntos judiciales relacionados C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger entre otros ECLI:EU:C:2014:238.

30 Esta reclamación se puede ver en SVRV (2016, página 46 y siguiente).

consumidor es sumamente mala, como ha constatado el Global Privacy Enforcement Networks GPEN en su estudio „Barrido de privacidad“ en más de 300 aparatos del internet de las cosas.[31] Esto ha quedado también demostrado en el análisis de Mundo digital, un observador del mercado, „Dispositivos que se llevan puestos (wearables), aplicaciones para mantenerse en forma y protección de datos: ¿todo bajo control?“[32]. Un análisis ejemplar de una aplicación utilizada en el internet de las cosas ha arrojado, además, que algunas cláusulas conformes a los artículos 307 y 308 del BGB [Código civil alemán] podrían no tener validez dado que imponen a los consumidores obligaciones de verificación y control unilaterales respecto a la modificación de las cláusulas perjudicando de forma inapropiada a los consumidores por la falta de esclarecimiento sobre la transmisión de datos a terceros (Domurath & Kosyra, 2016).

De esto se deduce la necesidad imperiosa de actuar de cara a la transparencia y legalidad de las CGC y declaraciones en materia de protección de datos. La demanda regulatoria de „una sola página“, que se está elaborando en un proceso con sectores interesados bajo la dirección del BMJV, podrá contribuir a lograr la transparencia y la legalidad exigidas porque va más allá de la idea de una sola página expuesta en el marco de la Cumbre Nacional de TI de 2015[33], que se refiere exclusivamente a las informaciones sobre protección de datos.

31 Se pueden encontrar más informaciones en la página web del responsable irlandés en materia de protección de datos (consultado el 14 de junio de 2017 en el URL https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm). En Alemania participaron el representante regional de protección de datos de Baden-Württemberg y la Oficina regional de Baviera en materia de vigilancia de la protección de datos.

32 En nueve de doce dispositivos que se llevan puestos (wearables) analizados se pudieron observar considerables infracciones contra la Ley en materia de protección de datos y la organización de protección de los consumidores de Renania del Norte-Westfalia envió una reclamación a los oferentes (Moll et al., 2017).

33 Una muestra de esa protección de datos de una sola página ha sido elaborada por la plataforma „Protección de los consumidores en el mundo digital“ dirigida por el BMJV y formada por representantes de la política, la economía, la ciencia, las organizaciones de consumidores y de protección de datos e instituciones del sector jurídico.

5.2. Revelar algoritmos y permitir que sean verificables

El SVRV reafirma la recomendación[34] de asegurar mediante normas legales (a) que los algoritmos tengan en cuenta las normas de los derechos del consumidor, del derecho en materia de protección de datos, del derecho en materia de antidiscriminación y de la seguridad digital, así como hacer transparentes los parámetros en los que se basan los algoritmos que estén en contacto directo con los consumidores, (b) que mediante la obligación estandarizada de revelar informaciones se revelen los algoritmos a un círculo de expertos que, mediante la toma de pruebas al azar, verifiquen la seguridad legal. El SVRV recomienda desarrollar estándares legales y depositar de forma duradera los códigos fuente.

La revelación de algoritmos para un círculo de expertos (por ejemplo, la agencia digital exigida por el SVRV) es decisiva para cumplir las normas legislativas cuando se trata de decisiones automatizadas mediante algoritmos. Aquí se trata, especialmente, de los derechos del consumidor, la antidiscriminación y la lealtad de las prácticas comerciales, pero también el cumplimiento de principios fijados respecto al derecho en materia de protección de datos, principios como el ahorro de datos e imputación a fines específicos. Para los consumidores mismos es importante, sobre todo, conocer los parámetros en los que se basan los algoritmos (como las variables y su ponderación) porque solamente así pueden presentar objeciones. Estas tareas podrían concentrarse en una agencia digital. Una agencia de este tipo es necesaria para asentar allí las pericias sobre la verificación del cumplimiento de las normas legislativas.

El empleo de algoritmos y el previsible perfeccionamiento de los algoritmos de aprendizaje automático en un mundo que sigue conectándose permanentemente afectan los principios éticos profundamente arraigados en nuestra convivencia social. Las cuestiones éticas reclaman una función de orden por parte del dere-

34 Esta reclamación se puede ver en SVRV (2016, página 67).

cho que no puede negarse a esbozar normativas al respecto. Un desafío especial radica en dar respuesta a la pregunta de cómo se puede asegurar con medios legales que los algoritmos de aprendizaje automático "actúen" con responsabilidad ética. Queda claro que, si bien la política jurídica puede contar con las experiencias de aquellos que impulsan el desarrollo de la Inteligencia Artificial (IA) (en ese sentido: BMWi, 2017b) sin embargo, el cumplimiento de estándares regulativos no puede basarse exclusivamente en la competitividad o la responsabilidad ética de la industria. Pero ¿cómo puede insertarse en la normativa un proceso que se autodirige?

En primer lugar, es necesario aclarar que el control de algoritmos puede tener lugar en diversos niveles. Se pueden controlar las fórmulas matemáticas mismas, pero también los parámetros considerables para la decisión o el resultado de la calculación o apreciación en la que se basan. Para los derechos del consumidor se pueden introducir, por ejemplo, condiciones para el control de los parámetros de algoritmos que no solamente se derivan del derecho de las condiciones generales de contratación (véase 5.1.) y de las condiciones de la seguridad informática (véase 3.3.), sino también del derecho en materia de antidiscriminación, lealtad y protección de datos. En este caso se trata, por un lado, de los parámetros con los que se mide la legitimidad de las decisiones tomadas a través de algoritmos y, por otro lado, se trata del control humano de esas decisiones.

Los requisitos del derecho en materia de antidiscriminación[35] como así también del derecho en materia de la lealtad de las prácticas comerciales[36] deben ser tenidos en cuenta, especialmente cuando los consumidores se ven confrontados con decisiones automatizadas. Puesto que con la ayuda de algoritmos es posible diseñar publicidad, ofertas, precios y también contratos de forma aparentemente individual, a pesar de que detrás de la individualización se puede esconder una discriminación. Esta discriminación no se orienta necesariamente a un individuo en particular, sino a un grupo de individuos que presentan características específicas determinadas a través de algoritmos (Angwin & Parris, 2016).

Además, los principios del ahorro de datos indicados en el derecho en materia de protección de datos (artículo 5 apartado 1 letra c del RGPD [Reglamento General sobre la Protección de Datos en la UE]) y de la imputación de los datos a fines específicos (artículo 5 apartado 1 letra b del RGPD) deben seguir siendo principios de conducta y tienen que ser tenidos en cuenta al emplear algoritmos. Solamente así se podrá lograr que los consumidores confíen en el manejo de datos personales por parte del Estado y la economía privada. Esto significa que los estudios que examinan de forma crítica la compatibilidad de grandes datos con esos principios (Helbing, 2015), así como la exigencia de un derecho a que los productos no recopilen datos (Becker, 2017) o a un „Derecho a un mundo análogo" (Maas, 2015)[37] deben discutirse seria y enérgicamente a nivel político. Se podría fomentar el desarrollo de productos y servicios cuyos algoritmos posibiliten la eliminación automática de datos (palabras clave: privacidad desde el diseño y privacidad por defecto).

También en el caso de algoritmos de aprendizaje automático se debería poder asignar la responsabilidad legal de los mismos. Para lograrlo, se deben seguir y, dado el caso, impulsar proyectos de investigación. Especialmente en el caso de algoritmos de aprendizaje automático los legisladores tendrían que aprovechar los conocimientos de las empresas especializadas en tecnología de la información y la comunicación, así como de los expertos en los respectivos campos de investigación y, sin debilitar las normas legales existentes, integrarlos en un proceso tendente a elaborar un código de conducta sobre el empleo de datos personales, sistemas de inteligencia artificial y el análisis de grandes datos.

35 Por ejemplo, la Ley general de Igualdad de Trato, artículo 19 apartado 1: 'No es admisible ningún perjuicio por razone de raza o procedencia étnica, por razones de género, religión, algún impedimento físico, edad o identidad sexual al constituir, realizar y finalizar relaciones obligatorias en Derecho civil (…)'. Respecto al Derecho de la UE: Directiva 2000/43/CE del Consejo del 29 de junio de 2000 sobre la aplicación de la Ley general de Igualdad de Trato sin diferencias de raza o procedencia étnica, OJ L 180/22, 19.7.2000 y Directiva 2004/113/CE del Consejo del 13 de diciembre de 2004 sobre la materialización del principio de igualdad de trato entre hombres y mujeres en el caso del acceso y la provisión de bienes y servicios, OJ L 373/37, 21.12.2004.

36 Véase Directiva 2005/29/CE del Parlamento Europeo y del Consejo del 11 de mayo de 2005 sobre prácticas comerciales desleales en el mercado comercial interno entre las empresas y los consumidores y sobre la modificación de la Directiva 84/450/CEE del Consejo, de las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo, así como del Reglamento (CE) no. 2006/2004 del Parlamento Europeo y del Consejo (Directiva sobre prácticas comerciales desleales) OJ L 149/22, 11.6.2005, que prohíbe prácticas comerciales desleales si contienen „datos falsos y, por lo tanto, incorrectos o si de alguna forma, …, incluso con datos correctos engañan al consumidor medio en lo que se refiere a uno o varios de los puntos precedentes o están en condiciones de engañarlo e inducirle de forma real o premeditada a tomar una decisión comercial que él no hubiera tomado.

37 Artículo 13 de los Derechos básicos digitales propuestos por Heiko Maas (consultado el 14 de junio de 2017 en el URL http://www.bmjv.de/SharedDocs/Interviews/DE/2015/Namensartikel/12092015_DieZeit.html).

El cumplimiento de esos parámetros solamente podrá ser verificado, si es posible, con la ayuda de una instancia estatal que obligue a las empresas a revelar datos y dar informaciones.[38] Para hacer justicia al interés de las empresas en mantener sus secretos comerciales, por un lado, y al derecho a la información de los interesados, por otro lado, (artículo 34 apartado 1 página 4 de la BDSG),[39] los algoritmos podrían revelarse a un círculo de expertos de una instancia estatal como por ejemplo, una agencia digital que verificara mediante pruebas al azar la ausencia de objeciones legales a la obligación estandarizada de revelar informaciones. Para ello se deberán desarrollar procedimientos estandarizados de ingeniería de software.

Teniendo en cuenta el hecho de que gran parte de las empresas más innovadoras especializadas en tecnología de la información y la comunicación se encuentran fuera de Alemania es imprescindible hacer una acción internacional concertada. El foro ideal para la búsqueda de soluciones adecuadas sería la Unión Europea, mejor aún la OCDE y las Naciones Unidas.

5.3. Mejorar el derecho a la información gratuita

El Consejo de Expertos recomienda garantizar el derecho a la información gratuita (artículo 34 de la BDSG) sin limitaciones, así como obligar a las empresas a informar a los consumidores de forma transparente, entendible y fácilmente reconocible sobre el derecho que ellos tienen a la información y a la posibilidad de rectificar datos erróneos al ofrecer sus productos (es decir rectificación, eliminación y bloqueo).

De momento, la implementación de la información gratuita está relacionada con considerables dificultades prácticas que reducen la efectividad de ese derecho fundamental para la sociedad digital. Los consumidores no están lo suficientemente informados sobre sus derechos y, además, tienen problemas al querer solicitar informaciones gratuitas. Para poder concientizar a los consumidores de forma efectiva sobre éste y otros derechos relacionados, el derecho a información no solamente debe estar incluido de forma ligeramente entendible y transparente en las páginas web, sino que, además, debe ser posible recibir de forma sencilla informaciones gratuitas. Por lo tanto, habría que discutir el comportamiento de las instancias responsables.

Según el derecho vigente, cuando entidades públicas y privadas recopilan datos sin que las personas afectadas tengan conocimiento de ello, se les debe informar sobre el almacenamiento, la entidad responsable, así como las finalidades del tratamiento de los datos (artículos 19a y 33 de la BDSG y artículo 15 del RGPD). Por otra parte, si el afectado así lo exige, la entidad responsable deberá informarle sobre los datos almacenados relativos a su persona, la procedencia de esos datos, los destinatarios de los datos y las razones del almacenamiento (artículos 19 y 34 de la BDSG y artículo 15 del RGPD).

El derecho a la información es la base para el ejercicio de los demás derechos de la persona afectada y, por lo tanto, el núcleo del derecho a la autodeterminación informativa. También refleja la idea de que, en última instancia, son personas las que toman decisiones y/o que también los algoritmos aplicados tienen que estar sometidos de forma permanente al control humano en lo que se refiere a sus decisiones. En ese sentido, el artículo 6 apartado 1 de la BDSG constata que las decisiones considerables desde el punto de vista legal no pueden basarse exclusivamente en el tratamiento automatizado de datos personales si esas decisiones sirven para la evaluación de características individuales de la personalidad. Al respecto, los artículos 21 y 22 del RGPD conceden un derecho de oposición. Además, el derecho a la información representa una posibilidad individual de control de los principios de reducción de datos y su imputación a fines específicos. Esto facilita de forma decisiva la transparencia a la hora de tomar decisiones automatizadas. Solamente cuando los afectados tienen conocimiento de la identificación y el almacenamiento de

38 Esta reclamación se puede ver en SVRV (2016, página 71).

39 En este sentido el BGH [Tribunal Supremo Federal Alemán] en la sentencia de la Schufa decidió que fórmulas de calificación de valoración de solvencia crediticia están protegidas en calidad de secreto comercial (BGH VI ZR 156/13). Actualmente, el caso se encuentra en el Tribunal Constitucional Federal Alemán. Aún no se conoce la fecha de la decisión.

datos se pueden rectificar los datos incorrectos, borrar los datos almacenados de forma ilícita y que ya no son necesarios para la finalidad indicada y bloquear los datos cuya exactitud o inexactitud no se pueda comprobar, en tanto su exactitud sea refutada por el afectado (artículos 20 y 35 de la BDSG y artículos 16 y 17 del RGPD).[40]

En este caso se trata también de solucionar el conflicto de intereses provocado por el deseo de eliminación de la persona afectada y el deseo de información de la persona que busca informaciones y/o el interés comercial de las empresas. Al respecto, el TJCE indicó en su sentencia en el caso Google[41] que el derecho de la persona afectada a poseer sus datos puede prevalecer, sin lugar a duda, al interés de información de la opinión pública. Sin embargo, la implementación del derecho a la supresión de datos y/o del „derecho al olvido", como se indica en el artículo 17 del RGPD, es problemática en la práctica a causa de las dificultades legales y técnicas. A pesar de que, en principio, la eliminación de datos es posible desde el punto de vista técnico, frecuentemente, está unida a un gran despliegue técnico (Weis et al., 2016). También es problemático el hecho de que la eliminación, muchas veces, solamente sea realizable „de forma parcial". Con frecuencia, los datos también siguen estando disponibles en otros dominios después de su eliminación. Por el contrario, los consumidores desconocen estas restricciones en la aplicación de la ley, por lo tanto, aquí se presenta una necesidad fundamental de aclaración. Se deben apoyar los planteamientos plausibles para imponer el derecho a la eliminación, dado el caso, se debe obligar a los oferentes en las redes sociales y otros servicios en línea a ofrecer opciones pertinentes a sus clientes.

Además, los afectados no saben, frecuentemente, cómo pueden ejercer en la práctica su derecho a la información, así como los derechos consiguientes. Muchas veces los consumidores no saben cuáles son las empresas que tratan sus datos. Spindler et al. (2016) constatan una „grave discrepancia" entre derechos y praxis. Además, las posibilidades de obtener informaciones de forma gratuita no están indicadas claramente en las páginas web, por el contrario, en el caso de la autoinformación de la Schufa [Asociación alemana de protección para garantizar la actividad crediticia general], por ejemplo, se envía a los consumidores primeramente a las páginas pagadas (Korczak, 2016). Hay también indicios que permiten suponer que las informaciones gratuitas tardan, frecuentemente, más tiempo que las pagadas (Korczak, 2016; Roßnagel et al., 2016).v

Se tiene que garantizar que las empresas que recopilan y tratan datos indiquen claramente en sus páginas web las posibilidades de obtener informaciones de forma gratuita y las ofrezcan de forma adecuada en publicaciones dirigidas a los consumidores. Por lo tanto, las empresas tendrían que estar obligadas a indicar claramente la posibilidad de obtener informaciones gratuitas. Habrá que discutir si es necesario exigir una responsabilidad para que se respete esa obligación y fortalecer las normas legislativas. Además, esa normativa tiene que aclarar ese derecho de forma fácilmente entendible, así como los derechos a rectificación, eliminación y bloqueo. En esta ocasión se hace hincapié en la demanda de que las declaraciones en materia de protección de datos, por un lado, deben ser puestas a disposición a los consumidores (véase demanda 5.1).

Por lo demás, también el control de algoritmos (véase demanda 5.2) tiene aquí importancia decisiva apoyando a los consumidores a mantener la transparencia sobre los datos recopilados por ellos porque puede contribuir a reducir la cantidad de datos. El control de algoritmos también puede ayudar a mitigar los problemas de los consumidores al imponer sus derechos.

40 Sobre los derechos a corrección: Becker (2017).

41 TJCE sentencia del 13 de mayo de 2014 en el caso C-131/12, Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, UE:C:2014:317.

5.4. Seguir desarrollando estándares mínimos para la interoperabilidad

El SVRV recomienda desarrollar estándares mínimos que garanticen una cierta compatibilidad entre los servicios digitales de forma tal que una comunicación entre las cuentas de usuario sea posible independientemente de los oferentes (interoperabilidad – de forma análoga a la telefonía móvil).

La interoperabilidad en el sentido de posibilidad de portabilidad de los datos accesibles para el usuario no se da, actualmente, de forma sistemática entre las redes sociales o servicios de mensajería. Se produce el denominado efecto de dependencia por cautividad que siempre conlleva el peligro de esconder alguna forma de abuso de poder de mercado, como se puede ver claramente en el mercado alemán en plataformas como Facebook y WhatsApp. Soluciones técnicas de interoperabilidad, como ya existen también entre los diversos oferentes de telefonía móvil, podrían presentar nuevos incentivos a la hora de competir.

El concepto de „interoperabilidad" toca la médula de la sociedad digital. En principio, interoperabilidad significa la posibilidad de transmitir datos a través de sistemas, aplicaciones y componentes y hacer que sean útiles (Palfrey & Gasser, 2012). Se trata del equilibrio entre dos dimensiones: por un lado, se han desarrollado con gran velocidad muchas nuevas infraestructuras que amplían la conectividad y las corrientes de datos entre individuos, organizaciones y sistemas; por otro lado, no existe hasta ahora ningún marco de orientación que defina los objetivos (sociales) de esa interoperabilidad y que gestione sus riesgos (Palfrey & Gasser, 2012). No sólo se trata de técnica y corrientes de datos, sino de una cultura de interacciones humanas e institucionales. Se pueden diferenciar cuatro capas diversas de la interoperabilidad que, al mismo tiempo, están relacionadas entre sí (véase al respecto Kominers, 2012; Gasser, 2012; Palfrey & Gasser, 2012): a nivel técnico se trata de la posibilidad de los sistemas técnicos de relacionarse entre sí, frecuentemente, mediante una interfaz acordada; segundo, a nivel de los datos y/o nivel semántico se trata de la utilizabilidad y legibilidad de los datos que se transmiten a través de la interfaz; tercero, la interoperabilidad solamente puede funcionar si los usuarios poseen las capacidades cognitivas y la predisposición necesarias para trabajar conjuntamente; por último, se trata en sentido abstracto de cooperaciones entre sistemas sociales como, por ejemplo, normas legales. Si la interoperabilidad tiene que ser aprovechable de forma efectiva deben hacerse, al mismo tiempo, reflexiones sociales.

De cara a las condiciones marco legales la interoperabilidad está regulada en Alemania y la UE a través de varios instrumentos, principalmente, en el sector de la telecomunicación. Desde septiembre se está actualizando la legislación de la UE en lo que concierne al marco de la estrategia del mercado digital con el objetivo de desarrollar una economía de datos y aumentar la competitividad (Comisión Europea, 2015). En general, la estandarización juega un papel decisivo al respecto. Conforme al artículo 17 de la Directiva marco[42], la Comisión Europea lleva la voz cantante en la elaboración de estándares no vinculantes en concepto de base para la prestación armonizada de servicios. Junto con el Comité Europeo para la estandarización impulsa, especialmente, el desarrollo de estándares sobre todo para prestaciones de servicios interoperables en el sector de finanzas, transporte, administración y sanidad electrónica.[43] Las autoridades nacionales de reglamentación deben crear impulsos para la aplicación de esos estándares (artículo 5 Directiva de acceso)[44], así como impulsar la implementación de estándares internacionales.

42 Véase por ejemplo, el considerando 9 y el artículo 17 de la Directiva 2002/21/EC del Parlamento Europeo y del Consejo del 7 de marzo de 2002 sobre un marco legal común para redes electrónicas de comunicación y servicios, OJ L 108, 24.4.2002, adaptado a través de la Directiva 2009/140/CE del Parlamento Europeo y del Consejo del 25 de noviembre de 2009 sobre la modificación de la Directiva 2002/21/CE sobre un marco legal común para redes electrónicas de comunicación y servicios de comunicación electrónicos, de la Directiva 2002/19/CE sobre el acceso a redes electrónicas de comunicación y las respectivas instalaciones, así como su interconectividad y de la Directiva 2002/20/CE sobre el permiso de redes y servicios de comunicación electrónicos OJ L 337/37, 18.12.2009.

43 Las informaciones sobre los estándares que están en desarrollo y los ya aprobados serán puestos a disposición por el European Committee for Standardization (consultado el 14 de junio de 2017 en el URL standards.cen.eu).

44 Directiva 2002/19/CE del Parlamento Europeo y del Consejo del 7 de marzo de 2002 sobre el acceso a redes electrónicas de comunicación y las respectivas instalaciones, así como su interconectividad, OJ L 108, 24.4.2002 adaptado a través de la Directiva 2009/140/EC del Parlamento Europeo y del Consejo del 25 de noviembre de 2009 sobre la modificación de la Directiva 2002/21/CE sobre un marco legal común para redes electrónicas de comunicación y servicios de comunicación electrónicos, de la Directiva 2002/19/CE sobre el acceso a redes electrónicas de comunicación y las respectivas instalaciones, así como su interconectividad y de la Directiva 2002/20/CE sobre el permiso de redes y servicios de comunicación electrónicos (Directiva de acceso).

Básicamente se trata, en principio, de crear las condiciones técnicas para la interoperabilidad. Los estándares necesarios para ello y las consecuencias que esto generará para la economía, los consumidores y el Estado se están discutiendo para todo el mercado der servicios y productos digitales y aquí especialmente también para el internet de las cosas (Zingales, 2015; Kominers, 2012). Sin embargo, la interoperabilidad, así como la posibilidad de portar datos entre los oferentes de forma accesible para el usuario como, por ejemplo, también redes sociales y servicios de mensajería es, actualmente, casi imposible. Se produce el denominado efecto de dependencia por cautividad que siempre conlleva el peligro de esconder alguna forma de abuso de poder de mercado (Cámara Baja del Parlamento alemán, 2016), como se ve claramente en el mercado alemán en el caso de las plataformas como Facebook y WhatsApp. Las transformaciones directamente tangibles para los consumidores pueden traer consigo, especialmente, una mejora de la interoperabilidad de las grandes empresas como WhatsApp y Skype. Por consiguiente, de la fijación de estándares en lo que se refiere a interoperabilidad sería de esperar una apertura del mercado también para oferentes nuevos e innovadores. Una equiparación de la regulación de esas grandes empresas a los oferentes de telecomunicación permitiría correspondientemente que el mercado fuera más justo y más abierto también para sectores ajenos a la interoperabilidad (BMWi, 2017b).

5.5. Concretizar el derecho a la portabilidad de los datos

El SVRV reafirma la recomendación de entender el derecho a la portabilidad de los datos como el derecho a rescisión de contrato y recomienda fijar un marco para poder cambiar entre los diversos oferentes (de forma análoga a las transacciones de pago digital).

El derecho a la portabilidad de los datos, entendido como la transmisión de datos al consumidor mismo o a otro oferente, depende decididamente de las condiciones técnicas. Al respecto, habrá que fijar un marco legal similar a las transacciones digitales de pago. Si el consumidor exige que se le devuelvan sus datos se debe interpretar como un derecho a rescisión de contrato. Las inseguridades actuales en lo que se refiere a la formulación en el artículo 20 del RGPD deberán ser eliminadas concediéndole de forma expresa al consumidor un derecho a rescisión de contrato.

A raíz de la sentencia del TJCE en el caso Google[45] se introdujo el derecho a la portabilidad de los datos en el artículo 20 del RGPD. Por consiguiente, la persona afectada tiene el derecho a recibir sus datos personales en un formato estructurado, usual y legible y transmitirlo a un responsable y/o hacer que se transmita técnicamente. El derecho a la portabilidad de los datos deberá permitirle al afectado transferir a otros oferentes de servicios perfiles en las redes sociales o cuentas de correo electrónico. Esto debe abarcar necesariamente también datos de terceros (conversaciones por correo electrónico, imágenes recibidas, etc.). Por lo tanto, el derecho a la portabilidad de los datos para el ejercicio de la soberanía digital en el sentido de la autodeterminación informativa es sumamente importante porque les da a los consumidores la posibilidad de escoger entre diversos oferentes de servicios digitales y cambiar de oferente.

Al mismo tiempo, el derecho deberá fortalecer también la competitividad, si bien esto es discutible. Las autoridades alemanas y francesas en materia de com-

45 TJCE sentencia del 13 de mayo de 2014 en el caso C-131/12, Google Spain SL y Google Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, UE:C:2014:317.

petitividad han constatado que empresas afianzadas tienen gran poder de mercado porque, entre otras cosas, poseen grandes carteras de clientes y bases de datos y, por consiguiente, una ventaja competitiva frente a otras empresas que no disponen de un volumen comparable o de una diversidad de datos comparable (Birnstiel & Eckel, 2016). Esto puede provocar el denominado efecto de dependencia por cautividad (Cámara Baja del Parlamento alemán, 2016; Schantz, 2016; Swire & Lagos, 2013). En esta ocasión no es necesario dilucidar si estos efectos son desfavorables para la competitividad a causa de las cambiantes preferencias de los consumidores y los modelos comerciales de las empresas[46]. Pero sí queda claro que el objetivo del derecho a la portabilidad de los datos es una parte imprescindible de la estrategia de la UE para un mercado interior digital para Europa (Comisión Europea, 2015).

La implementación del derecho a la portabilidad de los datos es indiscutible. Si bien, desde el punto de vista técnico algunos se muestran convencidos de que la portabilidad de los datos es posible en lo que concierne a la denominada web semántica (Bojars, et al., 2008)[47] en la literatura especializada técnica, sin embargo, no hay de momento todavía ningún estándar sencillo con cuya ayuda se pudiera definir qué se considera válido como formato de datos estructurado y "usual" y qué no (Swire & Lagos, 2013). Además, la portabilidad de los datos se vuelve problemática cuando afecta también datos de terceros o cuando el grado de su personalización no es claro (véase al respecto Schweitzer et al, 2016; BMWi, 2017b). De momento, los estándares existentes y previstos son todavía demasiado complicados (Swartz, 2013). Teniendo en cuenta lo anterior, el Grupo de trabajo de protección de datos contemplado en el artículo 29 ha convocado a los representantes de la industria y el comercio a trabajar conjuntamente en un set de estándares y formatos de interoperabilidad (Article 29 Data Protection Working Party, 2017). Sin embargo, la interoperabilidad no debe servir solamente en el momento particular para la transmisión de datos en el marco del cambio de oferente. En realidad, las redes sociales o los servicios de chat, por ejemplo, deberían posibilitar estándares comunes para la interoperabilidad entre los oferentes.

Desde el punto de vista técnico en materia de datos es necesario discutir si el derecho a la portabilidad de los datos es positivo para los consumidores. El derecho a la portabilidad de los datos podría llevar a que después de haber accedido una vez de forma ilegal a los datos sea posible seguir accediendo permanentemente a ellos dado que se accede a muchos datos de forma automatizada (Swire & Lagos, 2013). Por lo tanto, se debe lograr un equilibrio entre el derecho a la portabilidad de los datos y la seguridad de los datos.

En el derecho alemán en materia de protección de datos ya se puede concretizar el derecho a la portabilidad de los datos en el sentido del artículo 20 del RGPD (Cámara Baja del Parlamento alemán, 2016). Sin lugar a duda, se debe garantizar que el derecho a la portabilidad de los datos sea efectivo. En ese sentido, el derecho a la portabilidad de los datos tendría que entenderse desde el punto de vista jurídico obligacional como rescisión del contrato del consumidor para que los consumidores puedan exigir la devolución sin costes de sus datos en un formato usual, legible e interoperable o la eliminación de los mismos. De esta forma, los datos pueden ser traspasados a otro prestador de servicios por el consumidor mismo o por un prestador de servicios a otro (artículo 20 apartado 2 del RGPD). Independientemente de las controversias sobre la efectividad del derecho, esto sería razonable por lo menos para los consumidores que quisieran beneficiarse de la competitividad en el mercado y traspasar sus datos a otros oferentes.

46 Existen algunas señales que indican que, en determinadas circunstancias, los consumidores pueden preferir la interoperabilidad (por ejemplo, productos de Apple), véase Zittrain (2009). Además, hay empresas que están dispuestas a intercambiar sus datos de forma cooperativa a través de plataformas (por ejemplo, plugin de Facebook para páginas web), véase Swire & Lagos (2013). Sobre los modelos comerciales en cambio véase Pasquale (2015).

47 La primera propuesta se basa en Berners-Lee (2000).

Bibliografía

Angwin, J. & Parris, T. (2016). Facebook lets advertisers exclude users by race. ProPublica blog (28 de octubre de 2016). Consultado el 21 de junio en el URL Fehler! Hyperlink-Referenz ungültig..

Article 29 Data Protection Party (2017). Guidelines on the right to data portability. 16/EN WP no. 242 rev.01. Consultado el 14 de junio en el URL http://ec.europa.eu/informa-tion_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

Barr, R. (2010). Transfer of learning between 2D and 3D sources during infancy: Informing theory and practice. Developmental Review, 30, 128-154.

Becker, M. (2017). Ein Recht auf datenerhebungsfreie Produkte. JuristenZeitung, 72 (4), 170-181.

Berners-Lee, T. (2000). Semantic web on XML 2000 conference (diciembre de 2000), Washington DC.

Birkel, C., Guzy, N., Hummelsheim, D., Oberwittler, D. & Pritsch, J. (2014). Der Deutsche Viktimisierungssurvey 2012. Erste Ergebnisse zu Opfererfahrungen, Einstellungen gegenüber der Polizei und Kriminalitätsfurcht. In H.-J. Albrecht & U. Sieber (Hrsg.), Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht: Arbeitsberichte (p. 1-134). Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Birnstiel, A. & Eckel, P. (2016). Competition law and data. Wettbewerb in Recht und Praxis, 10, 1189-1195.

Bitkom (2015). Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlín: Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom).

BMELV (2007). Charta Verbrauchersouveränität in der digitalen Welt, Konferenz „Herausforderungen und Chancen in einer digitalisierten Welt: Beiträge der Verbraucherpolitik. Berlin: Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV [Ministerio Federal Alemán de Alimentación, Agricultura y Protección del Consumidor]).

BMWi (2015). Leitplanken Digitaler Souveränität. Berlin: Bundesministerium für Wirtschaft und Energie ([BMWi Ministerio Federal Alemán de Economía y Energía]).

BMWi (2016). Grünbuch Digitale Plattformen. Bundesministerium für Wirtschaft und Energie ([BMWi Ministerio Federal Alemán de Economía y Energía]).

BMWI (2017a). G20 Digital Economy Ministerial Conference: G20 Digital Economy Ministerial Declaration – Shaping Digitalisation for an Interconnected World. Bundesministerium für Wirtschaft und Energie ([BMWi Ministerio Federal Alemán de Economía y Energía]).

BMWi (2017b). Weißbuch Digitale Plattformen des BMWi. Bundesministerium für Wirtschaft und Energie ([BMWi Ministerio Federal Alemán de Economía y Energía]).

BMWi & BMJV (2015). Mehr Sicherheit, Souveränität und Selbstbestimmung in der digitalen Wirtschaft. Bundesministerium für Wirtschaft und Energie ([BMWi Ministerio Federal Alemán de Economía y Energía]) und Bundesministerium der Justiz und für Verbraucherschutz (BMJV [Ministerio Federal de Justicia y Protección al Consumidor]).

Bojars, U., Passant, A., Breslin, J.G. & Decker, S. (2008). Social network and data portability using semantic web technologies. In Proceedings of the BIS 2008 Workshop on Social Aspects of the Web (mayo de 2008), Innsbruck.

BSI (2016). Die Lage der IT-Sicherheit in Deutschland 2016. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI [Oficina Federal Alemana para la Seguridad en la Técnica de la Información]).

Buchner, B. (2006). Informationelle Selbstbestimmung im Privatrecht. Tübingen: Mohr Siebeck.

Bug, M., Kraus, M. & Walenda, B. (2015). Analoge und digitale Unsicherheiten: Neue Perspektive auf Kriminalitätsfurcht. DIW Wochenbericht, 12/2015, 280-287.

Bundeskriminalamt (2016). Cybercrime: Bundeslagebild 2015. Wiesbaden: Bundeskriminalamt [Oficina Federal de Investigación Criminal].

Bundesregierung (2014). Digitale Agenda 2014-2017. Berlin: Bundesregierung [Gobierno federal alemán].

Bundesregierung (2008). Verbraucherpolitischer Bericht der Bundesregierung 2008, Berlin: Bundesregierung [Gobierno federal alemán].

Bundesregierung (2016). Verbraucherpolitischer Bericht der Bundesregierung 2016, Berlin: Bundesregierung [Gobierno federal alemán].

Carstensen, T. (2015). Neue Anforderungen und Belastungen durch digitale und mobile Technologien. WSI Mitteilungen, 68, 187-193.

Christl, W. & Spiekermann, S. (2016). Networks of control, Facultas. Consultado el 16 de noviembre de 2016 von URL http://crackedlabs.org/en/networksofcontrol.

De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data. Gütersloh: Bertelsmann Stiftung.

Destatis (2016). Wirtschaftsrechnungen: Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien. In Statistisches Bundesamt (Hrsg.), Fachserie 15 Reihe 4 (p. 1-45). Wiesbaden: Statistisches Bundesamt [Oficina Federal de Estadística].

Deutscher Bundestag (2016). Regulierung von Messengerdiensten: Datenportabilität und Interoperabilität. Wissenschaftliche Dienste no. WD 10 - 3000 - 060/16.

Döring, N. (2010). Sozialkontakte online: Identitäten, Beziehungen, Gemeinschaften. In W. Schweiger & K. Beck (Hrsg.), Handbuch Online-Kommunikation (p. 159-183). Wiesbaden: VS Verlag für Sozialwissenschaften.

Domurath, I. & Kosyra, L. (2016). Verbraucherdatenschutz im Internet der Dinge. Sachverständigenrat für Verbraucherfragen Working Paper no. 3. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Ellis, Y., Daniels, B. & Jauregui, A. (2010). The effect of multitasking on the grade performance of business students. Research in Higher Education Journal, 8 (1), 1-11.

Europäische Kommission (2015). Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) no. 192final.

Feierabend, S., Plankenhorn, T. & Rathgeb, T. (2016). JIM 2016: Jugend, Information, (Multi) Media. Stuttgart: Medienpädagogischer Forschungsverbund Südwest.

Ferrara, E., Varol, O., Davis, C., Menczer, F. & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59 (7), 96-104.

Friedewaldt, M., Lamla, J. & Roßnagel, A. (2017). Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer Fachmedien Wiesbaden GmbH.

Friedrichsen, M. & Bisa, P. (2016). Einführung – Analyse der digitalen Souveränität auf fünf Ebenen. In M. Friedrichsen & P-J. Bisa (Hrsg.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft (p. 1-6). Wiesbaden: Springer VS.

Gasser, U. (2012). Interoperability in the digital ecosystem, GSR Discussion paper. Cambridge, MA: The Berkman Center for Internet & Society at Harvard University.

Gigerenzer, G. (2010). Digitale Risikokompetenz. Enquete-Kommission Internet und digitale Gesellschaft, Ausschussdrucksache no. 17(24)014-F.

Gigerenzer, G. (2013). Risiko: Wie man die richtigen Entscheidungen trifft. München: C. Bertelsmann.

Gigerenzer, G. (2017). Digital risk literacy: Technology needs users who can control it. Scientific American (25 de febrero de 2017). Consultado el 20 de junio de 2016 en el URL https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

Gigerenzer, G., Schlegel-Matthies, K. & Wagner, G.G. (2016). Digitale Welt und Gesundheit. eHealth und mHealth – Chancen und Risiken der Digitalisierung im Gesundheitsbereich. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen [Consejo de Expertos en materia de Asuntos del Consumidor].

Golder, S.A. & Macy, M.W. (2014). Digital footprints: Opportunities and challenges for online social research. Annual Review of Sociology, 40, 129-152.

Helbing, T. (2015). Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, Kommunikation & Recht, 145 (3), 145-150.

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van der Hofen, J., Zicari, R. V. & Zwitter, A. (2017). Will democracy survive big data and artificial intelligence? Scientific American (25 de febrero de 2017). Consultado el 20 de junio en el URL https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

Hutt, W.H. (1940). The concept of consumers' sovereignty. The Economic Journal, 50 (197), 66-77.

Initiative D21 (2016). 2016 D21-Digital-Index: Jährliches Lagebild zur Digitalen Gesellschaft. Berlin: Initiative D21.

Jentzsch, N. (2016). State-of-the-art of the economics of Cyber-Security and Privacy. IPACSO - Innovation Framework for ICT Security Deliverable no. 4.1.

Jentzsch, N. (2017). Gutachten: Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds. In: Stiftung Datenschutz (Hrsg), Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen (Teil C – p. 1-41). Leipzig: Stiftung Datenschutz.

Junco, R. (2012). In-class multitasking and academic performance. Computers in Human Behavior, 28 (6), 2236-2243.

Junco, R. (2015). Student class standing, facebook use, and academic performance. Journal of Applied Developmental Psychology, 36, 18-29.

Karaboga, M., Masur, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P. & Simo Fhom, H. (2014). White Paper Selbstdatenschutz. In P. Zoche, R. Ammicht-Quinn, J. Lamla, A. Roßnagel, S. Trepte & M. Waidner (Hrsg.), Schriftenreihe Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt (p. 1-48). Creative Commons 4.0 International Lizenz.

Kardefelt-Winther, D. (2014). A conceptual and methodological critique of internet addiction research: Towards a model of compensatory internet use. Computers in Human Behavior, 31, 351-354.

Kominers, P. (2012). Interoperability case study internet of things (IoT). Berkman Center Research Publication no. 2012-10. Cambridge, MA: Berkman Center for Internet and Society at Harvard University.

Korczak, D. (2016). Marktcheck Kostenloser Auskunftsanspruch von Verbrauchern bei Auskunfteien: Abschlussbericht der GP Forschungsgruppe. Düsseldorf: Verbraucherzentrale Nordrhein-Westfalen.

Kucharski, A. (2016). Post-truth: Study epidemiology of fake news. Nature, 540 (7634), 525-525.

Kühl, E. & Breitegger, B. (2016). Der Angriff, der aus dem Kühlschrank kam, Zeit online (24 de octubre de 2016). Consultado el 14 de junio en el URL http://www.zeit.de/digital/internet/ 2016-10/ ddos-attacke-dyn-internet-der-dinge-us-wahl.

Kultusministerkonferenz (2008). Ländergemeinsame inhaltliche Anforderungen für die Fachwissenschaften und Fachdidaktiken in der Lehrerbildung. Bonn: Sekretariat der Kultusministerkonferenz [Secretaría de la Conferencia Permanente de los Ministros de Educación y Asuntos Culturales].

Kultusministerkonferenz (2016). Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt". Bonn: Sekretariat der Kultusministerkonferenz [Secretaría de la Conferencia Permanente de los Ministros de Educación y Asuntos Culturales].

Loh, K.K. & Kanai, R. (2016). How has the Internet reshaped human cognition? The Neuroscientist, 22 (5), 506-520.

Maas, H. (2015). EU-Datenschutz-Grundverordnung: Datensouveränität in der digitalen Gesellschaft. Datenschutz und Datensicherheit-DuD, 39 (9), 579-580.

Mertz, M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C. & Woopen, C. (2016). Digitale Selbstbestimmung. Köln: Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres).

Möchel, E. (2016). Machtvolle Rückkehr der DDoS-Attacken, ORF.at (4 de octubre de 2016). Consultado el 14 de junio en el URL http://fm4v3.orf.at/stories/1773571/.

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C. & Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle? Düsseldorf: Verbraucherzentrale NRW.

National Highway Traffic Safety Administration (2015). Distracted driving 2015. Washington, DC.

Ofiera, J. (2016). Ein Ad-Blocker-Verbot ist keine Lösung – Ausgediente Geschäftsmodelle nicht künstlich am Leben erhalten. Consultado el 27.02.2017 en el URL https://www.piratenfraktion-nrw.de/tag/digitalisierung/.

Ophir, E., Nass, C. & Wagner, A. D. (2009). Cognitive control in media multitaskers. Proceedings of the National Academy of Sciences, 106 (37), 15583-15587.

Orange (2014). The future of digital trust: A European study on the nature of consumer trust, and personal data. Consultado el 14 de junio en el URL https://www.orange.com/en/con tent/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf.

Palfrey, J. & Gasser, U. (2012). Interop: The promise and perils of highly interconnected systems. New York: Basic Books.

Palmetshofer, W., Semsrott, A. & Alberts, A. (2016). Der Wert persönlicher Daten: Ist Datenhandel der bessere Datenschutz? Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Pasquale, F. (2015). The back box society – The secret algorithms that control money and information. Cambridge, MA: Harvard University Press.

Persky, J. (1993). Retrospectives: consumer sovereignty. The Journal of Economic Perspectives, 7 (1), 183-191.

Rau, H. (2016). Der Souverän – wir haben ihn längst zu Grabe getragen. In M. Friedrichsen & P.-J. Bisa (Hrsg.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft (p. 79-92). Wiesbaden: Springer VS.

Reisch, L., Büchel, D., Joost, G. & Zander-Hayat, H. (2015). Digitale Welt und Handel. Ver-braucher im personalisierten Online-Handel. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Riekmann, J. & Kraus, M. (2015). Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe. DIW-Wochenbericht, 82 (12), 295-301.

Rifkin, J. (2014). Die Null-Grenzkosten-Gesellschaft: Das Internet der Dinge, kollaboratives Gemeingut und der Rückzug des Kapitalismus. Frankfurt am Main: Campus Verlag Rosen.

Roßnagel, A., Nebel, M. & Geminn, C. (2016). Entgeltliche Auskunftsansprüche zu Score-Werten und ihr Mehrwert für den Verbraucher. Düsseldorf: Verbraucherzentrale Nordrhein-Westfalen e.V.

Rotondi, V., Stanca, L. & Tomasuolo, M. (2017). Connecting alone: Smartphone use, quality of social interactions and well-being, DEMS Working Paper Series no. 357.

Schantz, P. (2016). Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. Neue Juristische Wochenschrift, 26, 1841-1847.

Schleusener, M. & Hosell, S. (2015). Personalisierte Preisdifferenzierung im Online-Handel, Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Schwarzkopf, S. (2011). The political theology of consumer sovereignty: Towards an ontology of consumer society. Theory, Culture & Society, 28 (3), 106-129.

Schweitzer, H., Fetzer, T. & Peitz, M. (2016). Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen. ZEW Discussion Paper Series no. 16-042.

Spindler, G., Thorun, C. & Wittmann, J. (2016). Rechtsdurchsetzung im Verbraucherdatenschutz. Berlín: Friedrich-Ebert-Stiftung.

Spinney, L. (2017). How facebook, fake news and friends are warping your memory. Nature, 543 (7644), 168-170.

Stiftung Kind und Jugend (2017). Gemeinsame Pressemitteilung zur BLIKK-Studie. Consultado el 14 de junio en el URL http://www.stiftung-kind-und-jugend.de/ fileadmin/pdf/2017-05-29_PM_Blikk.pdf.

Süss, D. (2017, April). Medienpädagogik–Trends und Herausforderungen aus Sicht der Positiven Psychologie. In D. Süss & C. Trültzsch-Wijnen (Hrsg.), Medienpädagogik (p. 39-52). Baden-Baden: Nomos Verlagsgesellschaft.

SVRV (2015). Verbraucherpolitik in der digitalen Welt: Standpunkte des Sachverständigenrates für Verbraucherfragen. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

SVRV (2016). Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Swartz, A. (2013). Aaron Swartz's a programmable web: An unfinished work. In J. Hendler & Y. Ding (Hrsg.), Synthesis lectures on the semantic web: Theory and Technology (p. 1-54). San Rafael, CA: Morgan & Claypool.

Swire, P. & Lagos, Y. (2013). Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. Maryland Law Review, 72 (2), 335-380.

Thomée, S. (2012). ICT use and mental health in young adults. Effects of computer and mobile phone use on stress, sleep disturbances, and symptoms of depression. Dissertation thesis. University of Gothenburg.

Underwood, M.K. & Ehrenreich, S. E. (2017). The power and pain of adolescents' digital communication: Cyber victimization and the perils of lurking. American Psychologist, 72, 144-58.

van der Schuur, W. A., Baumgartner, S. E., Sumter, S. R. & Valkenburg, P. M. (2015). The consequences of media multitasking for youth: A review. Computers in Human Behavior, 53, 204-215.

Weis, R., Lucks, S. & Grassmuck, V. (2016). Technologien für und wider Digitale Souveränität. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Wineburg, S., McGrew, S., Breakstone, J. & Ortega, T. (2016). Evaluating information: The cornerstone of civic online reasoning: Executive Summary. Stanford History Education Group.

Wood, E., Zivcakova, L., Gentile, P., Archer, K., De Pasquale, D. & Nosko, A. (2012). Examining the impact of off-task multi-tasking with technology on real-time classroom learning. Computers & Education, 58 (1), 365-374.

World Economic Forum (2014). Rethinking personal data: Trust and context in user-centred data ecosystems. Geneva: World Economic Forum.

Young, K. & Abreu, C. (2011). Internet addiction. A handbook and guide to evaluation and treatment. Hoboken, NJ: John Wiley & Sons.

Zander-Hayat, H., Domurath, I. & Gross, C. (2016a). Personalisierte Preise. Sachverständigenrat für Verbraucherfragen Working Paper no. 2. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV [Consejo de Expertos en materia de Asuntos del Consumidor]).

Zander-Hayat, H., Reisch, L. A. & Steffen, C. (2016b). Personalisierte Preise: Eine verbraucherpolitische Einordnung. Verbraucher und Recht, 31 (11), 403-409.

Zingales, N. (2015). Of coffee pods, videogames, and missed interoperability: Reflections for EU governance of the internet of things. TILEC Discussion Paper DP no. 2015-026.

Zittrain, J. (2008). The future of the internet – and how to stop it. London: Allen Lane.

Consejo de Expertos en materia de Asuntos del Consumidor

El Consejo de Expertos en materia de Asuntos del Consumidor es un gremio que asesora al Ministerio Federal Alemán de Justicia y Protección al Consumidor (BMJV). Fue constituido en noviembre de 2014 por el Ministro Federal Alemán de Justicia y Protección al Consumidor, Heiko Maas. La tarea del Consejo de Expertos en materia de Asuntos del Consumidor es apoyar al Ministerio Federal Alemán de Justicia y Protección al Consumidor en la concepción de una política relativa al consumidor basada en conocimientos científicos teniendo en cuenta las experiencias recogidas en la práctica.

El Consejo de Expertos es un gremio independiente y tiene su sede en Berlín.

La Prof. Dr. Lucia Reisch ejerce la presidencia del Consejo de Expertos.