

<http://idp.uoc.edu>

## Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

# Presentación

En el presente monográfico recogemos algunas de las intervenciones realizadas en el marco del V Congreso de Internet, Derecho y Política, que bajo el título genérico de «Cara y cruz de las redes sociales» tuvo lugar el pasado mes de julio en Barcelona.

La elección del tema del congreso no resultó difícil. En efecto, la creciente popularidad y el uso intensivo de estas redes, cuyos usuarios se cuentan por cientos de millones en todo el mundo, ponen sobre la mesa un conjunto de cuestiones de marcado interés, tanto en el plano jurídico como en el politológico. Por una parte aparecen las ventajas de estas plataformas como nuevos medios de relación social, de interacción, de intercambio de información, de generación de comunidades y superación de distancias. Pero junto a los aspectos positivos y esperanzadores, es obligado notar los riesgos que en la práctica plantean las redes sociales en relación con determinados bienes jurídicos. Algunos de los más evidentes son los que se proyectan sobre el ámbito de la intimidad o sobre el adecuado control y protección de los datos personales. Muchos usuarios deciden hacer total o parcialmente públicos algunos datos sensibles de su vida personal, renunciando aparentemente a esferas de privacidad. Esa renuncia, sin embargo, difícilmente puede haber tenido en cuenta las consecuencias que quizás a largo plazo pueden derivarse de esa despreocupada diseminación de datos privados. En la medida de lo posible, las redes sociales deben diseñarse de tal modo que contribuyan a paliar los posibles resultados negativos anticipados inadecuadamente por los usuarios. Otros problemas se suscitan en el plano de la seguridad, la suplantación de la personalidad, amenazas, *cyberbullying*, y otros ataques y conductas censurables. Es preciso valorar cómo se puede hacer frente a este tipo de riesgos, no necesariamente en términos de producción legislativa, sino de incentivo a la adopción de buenas prácticas y códigos de conducta por parte de las plataformas, y de una concienciación de los usuarios que tenga en cuenta las motivaciones efectivas que les impelen a participar de modo intensivo y no siempre suficientemente reflexivo en estas redes.

Sobre éstas y otras cuestiones se trató y se debatió a lo largo de dos días en el V Congreso IDP, en el que se abordaron también las estimulantes experiencias de participación política y ciudadana que propician las redes. El texto que reproducimos del profesor Daithí Mac Síthigh, de la Universidad de East Anglia, ofrece bajo el título genérico de «Legisladores y políticos en el punto de mira» un panorama general de los temas tratados y de las sugerencias dirigidas, tanto a los operadores jurídicos como a los políticos, en relación con el uso de las redes sociales. Daithí Mac Síthigh fue el relator del Congreso, encargado de ofrecer al final de cada jornada una síntesis comentada de los principales aspectos abordados en las ponencias y suscitados en el subsiguiente coloquio.

Además del texto del profesor Mac Síthigh recogemos en este monográfico tres de las ponencias presentadas. La primera de ellas es la intervención de Ignacio Alamillo, que se centra en cuestiones de seguridad, y de modo particular, en las políticas públicas que se están desarrollando en esta materia. Se refiere en especial a las políticas dirigidas a promover entre los usuarios la «cultura de la seguridad», concienciando a los ciudadanos sobre los riesgos y vulnerabilidades de la red y facilitando la comprensión de los elementos clave en materia de seguridad. Aborda asimismo otras políticas

públicas genéricas como las referidas al análisis y gestión de riesgos, a los sistemas de acreditación de seguridad de productos y servicios a través de mecanismos de evaluación y certificación, o a la inversión en investigación y desarrollo en materia de seguridad. Analizando el caso concreto de las políticas públicas de seguridad en Cataluña, da cuenta de las previsiones del Estatuto de Autonomía de Cataluña en este campo, así como el Plan nacional de impulso de la seguridad de las TIC adoptado por el Gobierno de la Generalitat el 17 de marzo de 2009.

Franck Durmortier, investigador del Centre de Recherches Informatique et Droit (CRID) de la Universidad de Namur, analiza las interacciones de los usuarios en las redes sociales, estudiando en particular el caso de Facebook. Examina los incentivos presentes en esta red para que los usuarios revelen información real, actualizada y completa, de donde se derivan evidentes amenazas para su privacidad. Para Durmortier, la principal de estas amenazas estriba en el riesgo de descontextualización de la información proporcionada por los usuarios. Una amenaza que se cierne no sólo sobre el derecho a la protección de los datos personales, sino que afecta también a la privacidad en un sentido más amplio, considerada como el derecho del ser humano a erigirse en sujeto múltiple y contextual, con una identidad que es configurable de modo diverso en contextos distintos. Así, defiende el autor que el derecho a la privacidad puede caracterizarse como un derecho a la integridad contextual que garantice al sujeto la posibilidad de construir su propia identidad en relaciones diferenciadas, derecho que en un entorno como Facebook se ve directamente amenazado. Durmortier propone conceptualizar el derecho a la protección de datos como una herramienta para permitir a los sujetos comportarse como *dividuos contextuales*. Plataformas como Facebook vienen en la práctica a impedir esta *dividualidad* o multi-contextualidad al facilitar la recomposición de los datos fusionando los diversos contextos en uno solo. Para contribuir a paliar este riesgo, Durmortier, en línea con las recomendaciones del Grupo de Trabajo del artículo 29 contenidas en el *Working Paper* nº 163, de 12 de junio, señala la conveniencia de que las redes sociales establezcan por defecto una configuración máximamente protectora de la privacidad, habida cuenta de que es muy bajo el porcentaje de usuarios que se preocupa por modificar la configuración establecida por defecto. Sin embargo, se muestra escéptico ante la sugerencia apuntada en dicho documento de atribuir a los usuarios, en determinados supuestos, la condición de «responsables del tratamiento», puesto que la atribución de mayor responsabilidad a los usuarios no se ajusta al nivel real de concienciación de los ciudadanos en materia de protección de datos. Las soluciones, concluye, deben venir fundamentalmente de un diseño de la arquitectura de la plataforma que permita gobernar los flujos multi-contextuales de datos en la red social.

La privacidad en las redes sociales es también el foco de la ponencia de Antoni Roig, profesor de Derecho constitucional de la Universidad Autónoma de Barcelona. El profesor Roig muestra su preocupación por los riesgos tecnológicos que amenazan la privacidad, entre otros, el peligro que supone la captura de datos que el usuario ha revelado involuntariamente, y que pueden deducirse de los perfiles de las redes sociales mediante técnicas estadísticas y heurísticas. Estos riesgos se acrecientan con la Web 3.0 y las tecnologías de web semántica. Frente a estas amenazas, las soluciones jurídicas basadas estrictamente en la protección de los datos de carácter personal resultarán a su juicio insuficientes, ya que las nuevas herramientas permitirán obtener información personal a partir de datos aparentemente inocuos muy alejados del concepto legal de dato de carácter personal. Para afrontar estos riesgos el profesor Roig apuesta por el desarrollo y la implantación de tecnologías garantes de la privacidad (*privacy enhancing technologies*, PET), buscando de este modo soluciones tecnológicas a un problema marcadamente tecnológico. Entre estas soluciones destacan las protecciones contra la explotación de datos, o *privacy-preserving data mining* (P2DM), que trata de evitar que en los análisis estadísticos se revele información personal de los usuarios. Otras tecnologías se orientan a la protección de los pseudónimos, para evitar que de los mismos pueda deducirse la identidad real del usuario, y a la vez a permitir sistemas de reputación fiables. Concluye su ponencia destacando que

la protección actual de la privacidad en las redes sociales no es hoy por hoy satisfactoria, a pesar de los esfuerzos realizados y las recomendaciones propuestas por los grupos de expertos y agencias de protección de datos. Las protecciones tecnológicas garantes de la privacidad contribuirían notablemente a aliviar los riesgos y a hacer posible un derecho efectivo a la privacidad.

Miquel Peguera Poch

Profesor de Derecho mercantil y de Derecho y nuevas tecnologías de la UOC