UNIVERSITAT DE BARCELONA

Plan docente de la asignatura

Datos generales

Nombre de la asignatura: Seguridad, Tecnologías y Exclusión Social

Código de la asignatura: 570202

Curso académico: 2017-2018

Coordinación: Diego Torrente Robles

Departamento: Departamento de Sociología

Créditos: 2,5

Programa único: S

Consideraciones previas

La sociedad contemporánea es dinámica, compleja, interconectada y tecnológica. La tecnología está presente tanto en la vida colectiva como en la de las personas. Pero la tecnología tiene múltiples implicaciones. Por un lado, es un potente motor del cambio social, de la economía o del conocimiento. Nos ayuda a adaptarnos y a controlar los entornos. Nos soluciona problemas. Extiende los sentidos y las fuerzas humanas dándonos nuevas potencialidades. Por otra parte, su desarrollo, acceso y control la conecta con las dinámicas de conflicto social, relaciones de poder, y situaciones de discriminación y exclusión social. La evolución de la tecnología está condicionada por los cambios sociales y políticos y, al mismo tiempo, también es un motor de estos cambios. La propia lógica de progreso tecnológico, que conlleva efectos positivos, también implica riesgos asociados. Al mismo tiempo, la tecnología mantiene la promesa de ofrecernos respuestas para hacerles frente. Es la gran paradoja de la sociedad del riesgo. Todas estas cuestiones, y otras, hacen que el estudio de la relación entre tecnología, sociedad y seguridad sea un tema central en la sociología contemporánea.

El objetivo del curso es explorar las relaciones a tres bandas entre sociedad, tecnología y seguridad. En primer lugar, se estudia la relación entre tecnología y sociedad. En particular, interesan los vínculos entre cambio social y desarrollo tecnológico, así como las consecuencias sociales de la tecnología. En segundo lugar, se analizan las dinámicas entre sociedad y seguridad. Se presentan los principales problemas de seguridad de las sociedades avanzadas. Se presta atención a los planteamientos de la sociedad del riesgo como marco de análisis. En tercer lugar, se estudian las vinculaciones entre la tecnología y la seguridad. Se ve la primera como un factor creador de seguridad, y también de riesgo. Se discuten los delitos vinculados a internet, los debates en torno a su regulación y las principales estrategias de control por parte de la policía y otros agentes. También

se estudia la cuestión de la vigilancia, sus modalidades y algunas de las cuestiones relacionadas con los derechos. El curso se interesa por un amplio abanico de tecnologías, pero se centra más en las tecnologías de la información, las comunicaciones, la detección o la imagen aplicadas al campo de la seguridad ciudadana.

Horas estimadas de dedicación	**Horas totales 62,5**

Actividades presenciales	18
- Teórico-práctica	18
Trabajo tutelado/dirigido	20
Aprendizaje autónomo	24,5

Recomendaciones

Es necesaria una buena comprensión del inglés escrito para poder leer los materiales del curso.

Competencias que se desarrollan

— Capacidad para entender la naturaleza de la relación entre sociedad y tecnología.

— Capacidad para tener una visión global de los problemas de seguridad contemporáneos.

— Capacidad para analizar el rol de la tecnología en la seguridad.

— Capacidad para buscar fuentes, artículos y datos relevantes y actuales en esta área.

— Capacidad para redactar informes y presentarlos en público.

Objetivos de aprendizaje

Referidos a conocimientos

El objetivo general del curso es explorar el triángulo de relaciones entre sociedad, tecnología y seguridad, con una especial atención a los procesos de desigualdad derivados. La extensión de la materia y la duración del curso hacen que la asignatura tenga un carácter introductorio. El curso está pensado para presentar e introducir los grandes términos, y dar algunas herramientas al estudiante para que continúe profundizando por su cuenta. Los tres objetivos del curso son:

— Estudiar la relación entre el cambio social y el tecnológico.

— Estudiar las conexiones entre el cambio social y los problemas de seguridad.

— Estudiar los vínculos entre seguridad y tecnología.

Bloques temáticos

1. Tecnología y sociedad

** El bloque introduce qué es y qué hace la tecnología. Se da una visión general de las diferentes teorías sobre la relación entre tecnología y sociedad. Se presentan las ideas de Marx, Benjamin, Adorno, Baudrillard, Goffman, Foucault, Beck, Bauman, Khun o Castells. Se analiza cómo la sociedad da forma a la tecnología. Esta refleja los valores y objetivos sociales, económicos, militares y políticos de cada momento. Por otra parte, la tecnología se diseña para hacer cosas. En este sentido, se estudian sus usos y su repercusión social. Se analizan aspectos positivos como el papel en el crecimiento económico, la mejora en el acceso y participación en los servicios, las mayores posibilidades de interacción social, movilización política o como extensión de la educación y el conocimiento. También se plantean los aspectos negativos tales como la exclusión social, las barreras de acceso, el control social o la generación de riesgos. Se dan ejemplos del mundo laboral, la educación o la administración pública. Se estudia también la construcción social de la tecnología como contraposición al determinismo tecnológico. Finalmente, se explora la relación entre los usuarios y la tecnología en cuestiones como la identidad.*

1.1. Concepto de *tecnología*

1.2. Sociedad y avance científico y tecnológico

1.3. Impacto social de la tecnología

2. Sociedad y seguridad

** El bloque temático introduce la relación entre el cambio social y los problemas de seguridad que afrontan las sociedades contemporáneas. Para empezar, se presentan los conceptos de seguridad y riesgo, así como sus dimensiones. Se mencionan las teorías sociales que plantean la relación entre sociedad y riesgo. Se discuten algunos procesos sociales y su repercusión en la delincuencia común, la violencia interpersonal, la delincuencia organizada y la delincuencia del Estado, organizaciones y profesiones. La existencia de una sociedad mundial en red donde la información, las comunicaciones, las relaciones sociales, los servicios y el funcionamiento institucional están interconectados*

crea riesgos formidables. La competencia internacional en un mercado global presiona, a menudo, las organizaciones hacia prácticas cuestionables. Un sistema financiero nada regulado introduce incertidumbre y caos en la vida económica. Las instituciones políticas tienen márgenes de actuación limitados y afrontan crisis de legitimidad. El cambio climático, aparte de los problemas medioambientales que genera, altera las relaciones geopolíticas y económicas y genera nuevos conflictos.

2.1. Concepto y dimensiones de la seguridad

2.2. Sociedad red y riesgo

2.3. Análisis del riesgo

2.4. Consecuencias de la sociedad del riesgo

3. Seguridad y tecnología

** El objetivo de este bloque es estudiar el rol de la tecnología como medio y objeto de la delincuencia, así como el uso que se hace de la misma para controlarla y crear seguridad. Se da una visión general de la criminalidad en internet. Se habla de hackerismo, ciberterrorismo, piratería, fraude, acoso, pornografía y pederastia. Se discute la cuestión de la regulación y del control de internet y las dificultades de las respuestas policiales. Otro eje es la cuestión de la vigilancia. La vida de los individuos está bajo constante vigilancia: grabados por cámaras en la calle, geolocalizados por el móvil, rastreados por las galletas (cookies) de internet o espiados por las grandes agencias de seguridad. Se estudia dónde se da, a quién afecta y por qué se vigila. Se habla de los conceptos de privacidad, anonimato y confianza. Se discute el alcance de los riesgos de violación de derechos como el de la intimidad, el honor, la confidencialidad y la privacidad de las comunicaciones, o el control de la información personal (derecho al olvido). Se aborda la cuestión de la percepción de riesgos por parte de los usuarios de las tecnologías, la responsabilidad de su protección, y los conflictos y luchas por el control tanto de la información como de la seguridad de la misma.*

3.1. Tecnología y delincuencia

3.2. Los delitos en internet

3.3. Tecnología y seguridad

3.4. Vigilancia

Metodología y actividades formativas

La asignatura es una optativa de 2,5 créditos. Cada semana hay una hora y media de clase presencial. Hay previstos doce días de clase en el segundo semestre. El temario del curso se organiza en tres bloques y once temas (uno por semana). El planteamiento metodológico del curso se basa en leer, discutir y experimentar. El profesor hace una introducción al inicio de cada bloque para situar la temática que se trabaja en cada uno de ellos. El resto de las sesiones se desarrollan mediante la presentación, por parte de los estudiantes, de lecturas y otros datos sobre el tema que toque. Como

materiales de curso hay una selección de artículos clave de lectura obligatoria. Además, de cada tema, hay una selección breve de artículos específicos.

Cada tema se asigna a un estudiante (o más), que se compromete a profundizar en él durante el curso. Como los temas son muy amplios, trabajan algún aspecto específico que acuerdan con el profesor. La preparación del tema implica documentarse, buscar datos, leer artículos y hacer una presentación de los resultados en público en clase. La presentación debe incluir, como mínimo, referencias a un artículo o libro de la bibliografía que se facilita en el curso para este tema, o bien elegir otra lectura fundamental que se acuerda con el profesor con antelación. La presentación en público debe acompañarse con datos, gráficos, vídeos o cualquier otro recurso que ayude a llevar una realidad determinada en la clase. Estos recursos deben ser relevantes para entender el problema estudiado y las lecturas en las que se fundamenta.

Se incentiva que las presentaciones estén conectadas con la realidad y recojan aspectos prácticos. Para ilustrar el tema elegido se pueden utilizar diferentes recursos: hacer pequeñas búsquedas en internet, plantear supuestos de seguridad y riesgos, analizar datos de encuestas (por ejemplo, sobre hábitos de uso y de seguridad en internet), realizar análisis de riesgos, hacer observaciones sobre sistemas de videovigilancia, de control de perímetros y accesos, explicar el funcionamiento de un sistema de información geográfica o de reconocimiento facial, explicar los riesgos de la geolocalización en los móviles, realizar análisis de redes sociales tipo Facebook, etc.

Evaluación acreditativa de los aprendizajes

El curso requiere una presencia mínima del 80 %. La evaluación del curso se realiza mediante dos elementos. El primer elemento es la redacción de un informe final sobre el tema que ha trabajado el estudiante durante todo el curso y del que ha hecho una presentación en público. El estudiante va trabajando en él a lo largo del curso y debe entregarlo al final. En el Campus Virtual existe un protocolo sobre qué se evalúa y los contenidos mínimos. Esta prueba vale un 60 % de la nota.

El otro elemento de evaluación es un comentario personal en un foro del Campus Virtual sobre cada clase. Deben hacerse un mínimo de cinco comentarios. Estos comentarios deben incluir reflexiones sobre las discusiones llevadas a cabo en clase o hacer nuevas aportaciones. También se puede interactuar con otras aportaciones de los compañeros. Se evalúa la calidad en función de que se hagan citas de lecturas del programa (en particular las obligatorias) u otras relevantes, o que se aporten evidencias en forma de datos. La contribución a los foros vale un 40 % de la calificación final. Se tiene en cuenta la participación activa en clase.

Evaluación única

La evaluación única debe solicitarse en los plazos y forma que establece la coordinación del máster. Dentro de esta modalidad, el único elemento de evaluación es la recensión de cinco de las lecturas obligatorias del curso que constan en el Campus Virtual. Los criterios para hacer las recensiones y para evaluarlas constan en el Campus Virtual.

Fuentes de información básica

Libro

Beck, Ulrich (1992). *Risk society: towards a new modernity*. Collection Theory, culture and society. London: Sage.

Torrente, Diego (2001). *Desviación y delito*. Colección Manuales del Libro universitario; 65. Madrid: Alianza.

Clarke, Ronald V. (ed.) (1997). *Situational crime prevention: successful case studies.* 2nd ed. Guilderland (New York): Harrow and Heston.

Torrente, Diego (2015). Análisis de la seguridad privada. Barcelona: Editorial UOC.

Ball, Kirstie; Haggerty, Kevin D.; Lyon, David (eds.) (2012). *Routledge handbook of surveillance studies*. Abingdon, Oxon (United Kingdom): Routledge.

Jewkes, Yvonne; Yar, Majid (eds.) (2012). *Handbook of Internet crime*. Abingdon (United Kingdom): Routledge.

Lyon, David (2007). *Surveillance studies: an overview.* Cambridge (United Kingdom); Malden (Massachusetts, USA): Polity Press.

Kelling, George L.; Coles, Catherine M. (1997). *Fixing broken windows: restorign order and reducing crime in our communities*. New York: Touchstone.

Jones, Trevor; Newburn, Tim (1998). *Private security and public policing*. Collection Clarendon studies in criminology. Oxford (United Kingdom): Clarendon Press: Policy Studies Institute.

Khun, Thomas S. (1962). La estructura de las revoluciones científicas. Barcelona: fondo de Cultura Económica.

Louis Anthony Cox Jr. (2009). Risk Analysis of Complex and Uncertain Systems.Nueva York: Springer.

VV. AA. (2004). Políticas de seguridad ciudadana en Europa y América Latina: Lecciones y desafíos. Banco Interamericano de Desarrollo (BID).

Boyd, Danah Any:2012. Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon. Information, communication & society vol.:15 (5). Pàg.:662 -679.

Federal Trade Commission (USA) (2013). Internet of things: Privacy and Security in a connected world.

Bauman, Zygmunt (2014). After Snowden: Rethinking the Impact of Surveillance. International political sociology 8 (2). Pàg.:121 -144.

Artículo

Stiglitz, Joseph (2010). Risk and Global Economic Architecture: Why Full Financial Integration May Be

Undesirable. The American Economic Review 100 (2). Pàg.:388 -392.

Graham, S (2003). Digitizing surveillance: categorization, space, inequality. Critical social policy 23 (2). Pàg.:227 -248.

Castells, Manuel (2000). Materials for an exploratory theory of the network society. British Journal of Sociology 51 (1). pp. 5–24.

Galdón Clavell, Gemma; Hosein, Gus (eds.) (2012). "Privacidad y nuevas tecnologías: redes sociales, datos personales y tecnologías de vigilancia ante el reto del respeto a los derechos de las personas". *Novática: Revista de la Asociación de Técnicos de Informática*, núm. 217 (Mayo-Junio 2012), pp. 4-9.

Sylvia E. Korupp and Marc Szydlik (2005). Causes and Trends of the Digital Divide. European Sociological Review 211 (4).

Law, John (2008). On sociology and STS. The Sociological Review, 56:4.

Hekkert, M P (2007). Functions of innovation systems: A new approach for analysing technological change. Technological forecasting & social change:74 (4). Pàg.:413 -432.

Hekkert, M P (2007). Functions of innovation systems: A new approach for analysing technological change. Technological forecasting & social change:74 (4). Pàg.:413 -432.

Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, Fred D. Davis (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27 (3). pp. 425-478.

Crenshaw, M (1981). The causes of terrorism. Comparative politics 13 (4). Pàg.:379 -399.

Janette Webb (2012). Climate Change and Society: The Chimera of Behaviour Change Technologies. Sociology 46 (1) 109–125.

Zinn, Jens O. (2006). Recent Developments in Sociological Risk Theory. Forum: Qualitative Social Research 7 (1).

Adami, Christoph (2015). Artificial intelligence: Robots with instincts.. Nature 521 (7553). Pàg.:426 -427.

Lyon, D (2003). Technology vs 'terrorism': Circuits of city surveillance since September 11th. International Journal of Urban and Regional Research 27 (3). pp 666-78.

Jordan, T (1998). A sociology of hackers. The Sociological review 46 (4). Pàg.:757 -780.

Texto electrónico

Fundación telefónica (2011). Un mundo conectado: Las TIC transforman sociedades, culturas y economías.

World Economic Forum (2016). The Global Risks Report 2016. Ginebra: World Economic Forum.

OCDE (2011). Future Global Shocks. Improving risk governance.

Fundación telefónica (2013). El debate sobre la privacidad y seguridad en la Red: Regulación y mercados.

World Economic Forum (2016). The Impact of Digital Content: Opportunities and Risks of Creating and Sharing Information Online.

Revisado por los Servicios Lingüísticos de la UB.