

El concepto de surveillance. Aspectos éticos desde las ciencias de la información y la comunicación

Lic. Ariel Aguirre¹, Mgtr. María Elisa Martínez¹

¹Universidad de la República, Uruguay. Maestría en Información y Comunicación, PRODIC. E-mail:

ariel.aguirre@prodic.edu.uy

Resumen. Se analiza la problemática generada en torno al uso que presenta el concepto de *surveillance* para la ORC, desde la perspectiva ética que incluye dos visiones complementarias aportadas por las Ciencias de la Información y las Ciencias de la Comunicación. Se plantea el problema acudiendo a las definiciones generales y específicas del término, para luego analizarlo desde el punto de vista ético que incluye las visiones de los dos campos del conocimiento mencionados. Finalmente se reflexiona sobre los imperativos éticos que incluyen ambas visiones, concluyendo en la necesidad de mayor divulgación y jerarquización del problema planteado.

Introducción

Nos hemos propuesto discutir los aspectos más relevantes del concepto de *surveillance*, y su relación con las Ciencias de la Comunicación y la Información, en el marco de la ética referida a estos dos dominios científicos.

En la búsqueda de una definición de *surveillance* en la literatura, nos encontramos con textos que ponen énfasis en distintos aspectos de tal concepto. Sobre esto, Fuchs (2011a) aporta dos agrupamientos en torno a estos distintos énfasis: las definiciones generales, que mencionan aspectos tanto positivos como negativos del concepto; y las definiciones específicas, que se centran en los aspectos negativos.

Si damos por provisoriamente válido el planteo de Fuchs, en las definiciones generales el concepto se presenta como la recolección sistemática de información sobre humanos y humanos, destacándose como positivos los factores organizativos requeridos en toda sociedad y la capacidad o más bien la condición de lograr este propósito mediante la “vigilancia” de los sujetos. Como aspectos negativos, aparecen los vinculados a la limitación de las libertades individuales. En cambio, en las definiciones específicas, la tendencia es a convocar a los factores de dominación y control social, siendo la más difundida e influyente la que surge de la obra de Michel Foucault (1976). El efecto “neutralizador” y potencialmente desorientador de las definiciones generalistas es

cuestionado por este autor en favor de las específicas, que permiten construir categorías de análisis eficaces al distinguir “vigilancia” de “selección de información”, entre otros elementos. Esto, conlleva implicancias analíticas fundamentales, como veremos más adelante a través del análisis comparado de WikiLeaks y Wikipedia.

Un enfoque específico del término

Para poder entender el concepto de surveillance debemos revisar primero su definición. El Oxford Dictionary (2013) define **surveillance** como “*close observation, especially of a suspected spy or criminal*”; observar de cerca, especialmente a supuestos espías o criminales. El término remite directamente a una actividad policial, y es en ese sentido que se utiliza el término para definir la sociedad actual como “*surveillance society*” o sociedad de la vigilancia.

El concepto de *surveillance* puede relacionarse con los planteos de Michel Foucault (1976): la sociedad actual se vuelve cada vez más un panóptico o prisión ideal, donde todos estamos vigilados y donde nada escapa al ojo del vigilante. Foucault describió estas sociedades como *disciplinarias*, desarrolladas en los siglos XVIII y XIX, en las cuales el disciplinamiento se desarrollaba en todos los aspectos de la vida (escuela, hospital, cuartel, fábrica, prisión)

Esta *sociedad disciplinaria* se fue tornando según Deleuze (1991) en *sociedad del control* (futuro que Foucault había vislumbrado). En estas, nada se termina, todo está en constante cambio y movimiento, y el hombre pasó de integrar la dualidad masa-individuo, a integrar la dualidad datos-dividuos. El control es algo que se realiza a corto plazo, rápida y continuamente, mientras que la disciplina se realizaba a largo plazo, de forma lenta y discontinua. El control se instala de forma dispersa pero progresiva.

Una visión más cercana a nuestros tiempos la plantea Mattelart (2007). Este autor aporta que el concepto de Deleuze de “sociedad de control” se ha superado por un nuevo estadio social: en sus palabras “la *seguridad* se ha transformado en *obsesión por la seguridad*”. Esta transformación, impulsada por la implantación a escala global del capitalismo financiero y agravada tras los atentados del 11 de setiembre de 2001 (más precisamente por la declaración de guerra perpetua al terrorismo por parte de las superpotencias de occidente, especialmente Estados Unidos de América), provoca que

las sociedades de control se vayan tornando sociedades de sospecha; una sociedad donde los ciudadanos han ido cediendo espacios y derechos (individuales y colectivos) en aras de la seguridad perpetua, motivados e impulsados por el temor perpetuo que los distintos sistemas y agentes promotores de ésta visión de seguridad (tanto públicos como privados) se han encargado y se encargan constantemente de difundir, implementar y justificar.

Esta realidad se expresa de diversas maneras: la proliferación de sistemas cerrados de tv para vigilancia (tanto de lugares privados como públicos); el relacionamiento cada vez más fluido de bases de datos digitales que contienen la información de la interacción de las personas con el mundo; el masivo uso de perfiles individuales para acceder a las llamadas redes sociales, son algunos ejemplos. Otros, más mundanos y comunes son las interacciones continuas de los individuos con el aparato estatal: uso de bancos y sistemas financieros, sistemas de salud, de educación, de pensiones y planes jubilatorios, de planes de vivienda, etc. La interacción continua con el Estado (que desde la modernidad hasta nuestros días es el aparato de control por antonomasia utilizado por las élites en el poder) genera información que se registra en bases de datos, que a su vez son o pueden ser utilizadas para el control social.

Esta evolución de la sociedad del control no ha hecho más que exacerbar el fenómeno de *surveillance*. El concepto de *surveillance* se relaciona finalmente de manera previsible con el de *dataveillance* (vigilancia de datos, definida por el Oxford Dictionary (2013) como “*the practice of monitoring the online activity of a person or group*”) esta relación se establece cuando, en la necesidad de control absoluto, los gobiernos (ya sea directamente o a través de empresas privadas) establecen la vigilancia de la sociedad a través de los datos que los ciudadanos generan. Esta vigilancia se desarrolla no sólo controlando el uso masivo y social de bases de datos, sino más bien con la interacción de las mismas entre sí, y con la necesidad creciente por parte del aparato estatal de controlar la vida de sus ciudadanos a través de la vigilancia de los datos por ellos producidos.

La vigilancia social establecida en éstos términos tiene ventajas comparativas sobre planteos de vigilancia social anteriores: es menos visible a la vez que es más intrusiva; es más fácilmente desarrollable y viable desde el momento en que las personas están siendo educadas y formadas en el uso no sólo de las redes sociales, sino en toda la

infraestructura estatal de datos (haciendo énfasis en el uso de *datos*, y no de *información*), y desde el momento en que los datos son accedidos a través de infraestructura informacional basada en la electrónica de consumo, fácilmente vigilable por quienes detentan no sólo el monopolio del ejercicio de la fuerza, sino también una disponibilidad asimétrica de recursos respecto al ciudadano común.

Problemas éticos en el marco de las Ciencias de la Información

En el campo de la organización y representación del conocimiento (ORC) uno de los problemas fundamentales a resolver es cómo representar adecuadamente los conceptos registrados. Y decimos *adecuadamente* en el sentido de *adecuado al contexto y a las situaciones sociales e históricas en que dicha representación tiene lugar*.

Teniendo esto en cuenta, las elecciones que se realizan en este proceso no son ni banales, ni aleatorias, ni estáticas, ni eternas; dependen tanto de la formación de quien establece las elecciones, como del contexto en que estas se realizan. Y como tales, dichas elecciones pueden (y deben) ser revisadas según el contexto histórico: es esperable (y hasta deseable) que evolucionen o cambien con el tiempo.

Si partimos de estos supuestos, la relación que se establece entre los conceptos y su representación cobra una importancia enorme (y muchas veces vital) cuando se aplica al campo de la vigilancia, sea en el contexto de *surveillance* o en el de *dataveillance*. De esta manera, no será inocente representar contenidos con términos como “terrorismo”, “radicalismo islámico”, “radicalismo musulmán”, etc.

En el más notorio de éstos ejemplos (terrorismo), su definición según la Real Academia Española (2001) es “*1. Dominación por el terror. 2. Sucesión de actos de violencia ejecutados para infundir terror*”; siendo “terrorista” aquel “que practica actos de terrorismo”. La definición es bastante lineal, y no se agregan datos que contextualicen por lo menos el origen del término.

Según el Oxford Dictionary (2013) es “*the unofficial or unauthorized use of violence and intimidation in the pursuit of political aims*”; siendo “terrorista” “*a person who uses terrorism in the pursuit of political aims*”. El Oxford Dictionary agrega además el origen de la palabra “terrorist”, lo que genera el contexto para su comprensión.

En estos casos (estos ejemplos se pueden extrapolar a otros términos en éste u otro contexto) no sólo se debe tener en cuenta cual es el concepto a representar: se debe

conocer el significado real de los términos para aplicarlos, el contexto en el que nacen los términos; el contexto en el que se utilizan; etc.

Otro ejemplo claro es aquel donde se confunden términos que tienen significados diferentes aunque compartan una raíz común. No es lo mismo “integrismo islámico” que “radicalismo islámico” o “radicalismo árabe”, aunque muchas veces estos términos sean usados como sinónimos: mientras los dos primeros se refieren a movimientos o grupos relacionados con la religión islámica, el tercero se puede referir tanto a grupos naturales de Arabia; ó a hablantes del idioma árabe; ó a naturales específicamente de Arabia Saudita; por citar un ejemplo donde es común encontrar este tipo de “confusiones”.

Pero además del uso “correcto” o “exacto” del término que representa un concepto, habrá que tener en cuenta la intencionalidad en la representación de determinado concepto a través de determinado término, siempre que hablemos en términos de ética en ORC. “Terrorista islámico” y “terrorista árabe” no son necesariamente lo mismo, pero la visión que se transmite en occidente del fenómeno del terrorismo contemporáneo los mezcla y los transforma en uno, a través del etiquetado de “terrorismo”. Es más, bajo esta etiqueta se tiende a ubicar tanto a grupos terroristas árabes como a activistas sociales; a grupos guerrilleros de izquierda como a grupos de ultraderecha. El imperativo ético no es sólo *representar debidamente lo que es terrorismo* sino *no identificar como terrorista lo que no lo es*.

Las consecuencias del uso indiscriminado a nivel legal, social y/o político del término “terrorista” para definir todo aquello que se opone a determinado régimen (no existen definiciones claras de éste fenómeno) tiene consecuencias gravísimas en algunas partes del globo: el ejemplo más visible son los Estados Unidos, donde no existe una definición clara de “terrorismo” o “terrorista”, sirviendo el término para englobar casi cualquier forma de disidencia. En este sentido, no es menor la decisión de utilizar este término en contexto de la ORC.

Problemas éticos en el marco de las Ciencias de la Comunicación

WikiLeaks, autodefinida como “la primera agencia de inteligencia del pueblo”, posiblemente representa el fenómeno más interesante de los últimos tiempos, para

aplicar las categorías de análisis en torno al concepto de *surveillance*. Dice Fuchs (2011b), lúcidamente:

WikiLeaks makes information about organisations that abuse power available to the public by allowing the anonymous submission of secret documents that are analysed, summarised and presented in the WikiLeaks website. If WikiLeaks were understood as being a form of surveillance in the general neutral understanding of the term, then it could not be distinguished from other Internet projects like Wikipedia because both Wikipedia and WikiLeaks are systematic forms of gathering and assessing information, which is the core of neutral surveillance definitions. The difference, however, is that WikiLeaks is engaging in political struggles, is an explicitly politically motivated project, and wants to make information public that has to do with abuse of power.

En este enfoque teórico, existe una diferencia sustantiva entre dos proyectos. Por un lado, la selección y evaluación de la **información pública**, que podría ser el objeto de Wikipedia comparable al de cualquier otro proyecto enciclopedista tradicional, pero que se instala en la transgresión de erigir como autores calificados a los ciudadanos del mundo sin previo aval ni revisión de “expertos”, por la sola voluntad de aquellos en participar del proyecto colaborativo y bajo la premisa de una absoluta confianza en el poder colectivo de autorregulación y autocorrección. Por otro lado, el proyecto político de WikiLeaks que se posiciona como el dispositivo de “vigilancia” de los “vigilantes”, léase de las agencias de poder y control social, mediante la sustracción no autorizada de **información secreta** que deviene pública por esta vía. Pero no cualquier información, claro está, sino aquella que concierne esencialmente a la legitimidad social y autoridad intrínseca de las instituciones coercitivas y hegemónicas, por lo cual éstas ocultan del conocimiento público dicha información para perpetuarse en tal posición de poder. En este sentido, afirma Fuchs (2011, p. 7), podemos hablar en algunos casos de Internet “contra-vigilancia” porque *“powerful actors want to make their enemies and opponents visible, while they want to remain themselves invisible”*.

La cuestión central no estaría planteada, por lo tanto, en las categorías público/privado sino en el poder de decidir qué es privado y legítimamente protegido por el secreto, y qué debe ser expuesto al conocimiento de toda la sociedad. La pregunta es: ¿quién decide qué debe ser público?, ¿el Estado, las corporaciones, los individuos, las organizaciones sociales? El gobierno de los Estados Unidos afirma que las

publicaciones de WikiLeaks sobre acciones bélicas de ese país en Afganistán son “terroristas” porque vulneran su seguridad nacional, pero: ¿es el propio gobierno de EEUU el único que puede limitar qué le atañe a su soberanía y qué afecta a los intereses de otras naciones? ¿Puede WikiLeaks arrogarse ese derecho?

La misma cuestión se replantea en otros escenarios derivados de penetración de las Tecnologías de la Información y la Comunicación (TIC) en la vida cotidiana de la tercera parte de la humanidad. Una serie infinita de aplicaciones tecnológicas proveen a los usuarios de Internet de servicios de comunicación y entretenimiento que, amparados en los derechos de uso que todos aceptamos con un simple “clic” del *mouse* y nunca leemos, proceden a una discreta “vigilancia” de los usuarios en tanto consumidores finales, con el fin de iniciar, continuar o acrecentar la relación comercial. Se han divulgado preocupantes llamados de atención sobre los derechos vulnerados de los usuarios de las aplicaciones de Google, servicios de almacenamiento de archivos y redes sociales como Facebook, entre las más conocidas (Fuchs y Winseck, 2011, p. 259). Muchas veces estas voces de alarma, paradójicamente, han circulado de forma “viral” por los mismos medios cuestionados.

En estos casos, no se trata de información sustraída del secreto para hacerla pública y denunciar abusos o corrupción, sino de un procedimiento más complejo y silencioso. Estos servicios en la Web obtienen información sobre sus consumidores sistemáticamente a través de “software espía” pero legalmente cubierto (al aceptar aquellos los términos y condiciones de uso), pero de una forma que el usuario no puede conocer. Es decir, no puede saber qué y cuándo es observado por el sistema. A su vez, las empresas que operan estos servicios no vuelcan esta información privada directa y explícitamente en un ámbito público, sino que la procesan también secretamente como información estratégica para su modelo de negocios y plan de operaciones en el mercado. Eventualmente, podrían vender esta información a otras empresas sin que el consumidor tuviera conocimiento ni pudiera percatarse de ello.

Ninguna de estas preguntas puede ser respondida fácilmente. Lo seguro es que este escenario obliga a una profunda revisión de las acciones de los individuos y las organizaciones que actúan en el campo de la comunicación social.

Reflexiones finales

Como ya señalamos antes, el imperativo ético en el marco de la ORC es no sólo representar “adecuadamente” el conocimiento registrado, sino en combatir consciente y activamente las visiones neutralistas y ahistóricas que subyacen en la pretensión de representar el conocimiento de una vez y para siempre. En el caso del término “*surveillance*”, no creemos que sea innecesaria la acción que es definida por éste, sino que la misma se inscribe en un contexto determinado, y con motivaciones (a veces claras y otras no tanto) que deben necesariamente ser tenidas en cuenta para entender el fenómeno de manera cabal y saber qué es lo que se representa con éste término. Y más aún: en nuestro contexto es imperativo no sólo entender el fenómeno, sino tener en claro bajo qué intereses se desarrolla y qué se pretende que logre.

En la dimensión aplicada del campo de la comunicación, las implicancias éticas de los procesos de “vigilancia” plantean dilemas y conflictos a nivel de organizaciones y sujetos. Desde el ángulo de la construcción y empoderamiento de la ciudadanía, la penetración y desarrollo de las TIC ha derivado en nuevos escenarios prometedores desde el enfoque de la democratización en el acceso a la información y los medios de producción y circulación de información. Pero al mismo tiempo, se multiplican las preguntas en torno a la legitimidad y transparencia de los procesos de vigilancia de los estados y las corporaciones por un lado, y de los individuos y organizaciones sociales que abogan por la construcción de un contra-poder de vigilancia del poder.

Se requiere mayor divulgación y jerarquía de estas problemáticas en los ámbitos académicos y en su articulación con el campo profesional, para avanzar en el análisis de este estado de cosas que observamos pasivamente mientras se configura un escenario “orwelliano” en nuestras sociedades.

Referencias bibliográficas

- Deleuze, Gilles. 1991. Posdata sobre las sociedades de control. En: Christian Ferrer (Comp.) El lenguaje literario. Tº 2, Ed. Nordan, Montevideo.
- Foucault, Michel. 1976. Vigilar y castigar: nacimiento de la prisión. México, D.F.: Siglo XXI.

- Fuchs, Christian. 2011a. How to define surveillance?. *Matrizes* [en línea] 5 (1): 109-133. [Citado 28 Feb 2013]. Disponible en World Wide Web: <http://www.matrizes.usp.br/index.php/matrizes/article/download/203/347>
- Fuchs, Christian. 2011b. WikiLeaks: Power 2.0? Surveillance 2.0? Criticism 2.0? Alternative media 2.0? A political-economic analysis. *Global Media Journal – Australian Edition* [en línea] 5 (1). [Citado 28 Feb 2013]. Disponible en World Wide Web: <http://fuchs.uti.at/wp-content/uploads/wikileaks.pdf>
- Fuchs, Christian y Winseck, D. 2011. Critical media and communication studies today. A conversation. *TripleC*, vol. 9, nº 2, p. 247-271.
- Mattelart, Armand. 2007. *Un mundo vigilado*. Paris: La Decouverte.
- Oxford Dictionary. 2013. Dataveillance. En Oxford University Press. [Citado 26 Feb 2013]. Disponible en World Wide Web: <http://oxforddictionaries.com/es/definicion/ingles/dataveillance?q=dataveillance>
- Oxford Dictionary. 2013. Surveillance. En Oxford University Press. [Citado 26 Feb 2013]. Disponible en World Wide Web: <http://oxforddictionaries.com/definition/english/surveillance?q=surveillance>
- Oxford Dictionary. 2013. Terrorism. En Oxford University Press. [Citado 26 Feb 2013]. Disponible en World Wide Web: <http://oxforddictionaries.com/es/definicion/ingles/terrorism?q=terrorism>
- Real Academia Española. 2001. Terrorismo. En *Diccionario de la Lengua Española*. 22a ed. Madrid: Espasa Libros [Citado 26 Feb 2013]. Disponible en World Wide Web: <http://lema.rae.es/drae/?val=terrorismo>
- Real Academia Española. 2001. Terrorista. En *Diccionario de la Lengua Española*. 22a ed. Madrid: Espasa Libros [Citado 26 Feb 2013]. Disponible en World Wide Web: <http://lema.rae.es/drae/?val=terrorista>

Bibliografía consultada

- Roger Clarke. 1991. Information Technology and Dataveillance. En: Dunlop, Charles and Kling, Rob. *Computerization and Controversy: Value Conflicts and Social Choices*. Boston: Academic Press. UNESCO. 2005. *Hacia las sociedades del conocimiento*. UNESCO: París.