RELATORIA ETHICS AND TECHNOLOGY Controversies, Questions, and Strategies for Ethical Computing

Miguel Angel Caro

Universidad El Bosque

RELATORIA ETHICS AND TECHNOLOGY Controversies, Questions, and Strategies for Ethical Computing

Tavani(Tavani, 2011) comienza con responder la pregunta sobre, que es la privacidad personal, se debe partir que no existe en acuerdo universal en el concepto, sin embargo, entre los muchos conceptos en un sentido descriptivo se puede encontrar que, la privacidad se entiende como un depósito de información que puede ir disminuyendo, también puede entenderse como una zona que merece protección. Si se habla en términos legales, la privacidad es aquello que se puede violar, por lo tanto, para Tavani es importante distinguir entre privacidad en un sentido descriptivo como normativo. El enfoque principal en el capitulo 5 es examinar la privacidad de la información, sin embargo, también aborda las otras dos vistas de privacidad, la primera es la ausencia de intrusión y la segunda como un termino asociado con la libertad de interferencia en los asuntos personales.

La primera, privacidad de información, se ve como la capacidad de restringir el acceso y controlar su información personal. Para la segunda, Tavani nos introduce a Warren y Brandeis, para ellos la privacidad es un derecho legal en Estados Unidos; aunque no hay una descripción explicita de este derecho en las primeras 10 enmiendas, de la cuarta se puede inferir cierto derecho, protegiéndolos de la intrusión no gubernamental. el argumento de la privacidad como ausencia de intrusión se basa en el daño que se puede realizar a través del acceso físico de una persona o de sus posesiones. La última vista abordada por Tavani de la privacidad, es la libertad de interferencia, haciendo referencia a las decisiones y elecciones personales. Como ejemplo de esto, expone la decisión del tribunal que involucraba a Karen Ann Quinlan con su derecho a desistir de su soporte vital y tener el derecho a morir.

Para James Moor, los individuos tienen privacidad en una situación, entendiéndose como situación a cualquier tipo de actividad o relación, si y solo si esta protegido por las 3 vistas mencionadas previamente, intrusión, interferencia y acceso a la información. La teoría de Moor, hace una distinción entre tener privacidad y entre tener el derecho de privacidad. Para entender este punto Moore propone 2 escenarios, el primero es uno de

privacidad descriptiva, en donde Mary se encuentra en un laboratorio de la universidad trabajando a solas, cuando llega Tom y la ve trabajando en el computador; en este momento Mary perdió su privacidad natural, sin embargo, el laboratorio no es una zona normativamente privada. Para el segundo escenario, después de que Mary deja el laboratorio y llega a su casa, Tom la sigue y por la cerradura Tom observa a mary en su computador portátil, en los dos casos Tom ve a Mary interactuando con un computador, ya que nuestra vivienda se ha declarado normativamente privada como sociedad.

Para algunos críticos esta idea de privacidad es bastante amplia. por lo cual Tavani introduce el concepto de privacidad de Helen Nissenbaum, donde su modelo se basa en la integridad contextual, y para ello es necesario que se cumplan las normas de idoneidad y las de distribución, mientras estas dos estén presentes la persona conserva su privacidad, la idoneidad corresponde a si es apropiado o no divulgar una información dentro de un contexto, mientras que las normas de distribución se refieren a la limitación del flujo de información dentro y entre contextos.Existen dos posiciones con respecto al estado actual de la privacidad, tanto para Froomkin como para Garfinkel, hablan de la muerte de la privacidad, mientras que otros aun creen que se debe estar atento para preservar la poca privacidad que aun se pueda. Se podría entrar en el debate actual en donde para muchos milleninals, la privacidad no parece tener importancia, incluso tienen las ansias de compartir su información personal, sin embargo, en este capitulo se va a asumir que la privacidad tiene valor y es importante. Se hace difícil encontrar un consenso en las leyes y políticas de privacidad, ya que para muchas culturas no occidentales la privacidad no tiene mayor atractivo mientras que para las culturas occidentales sí.

para muchos la privacidad no hace parte de un valor intrínseco, para otros son valores instrumentales, sin embargo, para Fried, la privacidad es fundamental porque es un medio para ciertos fines, pero además es una condición para lograrlos. para Moore, la privacidad es una articulación a la seguridad. para Judith deCew el valor de la privacidad recae en la libertad e independencia, además protege de la presión de conformarse. Para otros autores, la privacidad es esencial para la democracia. De

acuerdo con esto se ve el valor que tiene en los bienes sociales, así como de autonomía y elección, lo cual merece la pena proteger, pero debido a las tecnologías cibernéticas esta privacidad se ve amenazada por tres diferentes prácticas, la recopilación de datos, el intercambio de datos y el procesamiento de datos.

En la recopilación de datos, se pueden encontrar los registros de las actividades que se realizan usando dispositivos electrónicos, que son capaces de monitorear a los individuos y grupos, un ejemplo de esto es la vigilancia del gobierno mediante las conversaciones telefónicas o las cámaras de video que monitorean los movimientos. La tecnología ha dado un gran cambio en la recolección de estos datos, en el pasado, era necesario contratar a una persona para monitorear el trabajo de un empleado, ahora estos registros son mas detallados con ayuda de los supervisores invisibles, los computadores. Otro medio de recopilación de datos es el uso de las cookies, en donde se registran las preferencias de navegación. Después de recolectar estos datos, se pasa al intercambio de estos, y en la actualidad existe un negocio en crecimiento que involucra la venta e intercambio de datos personales. Por último esta información puede ser fusionada, emparejada o minada, con el fin de aumentar la información o encontrar patrones que no sin visibles fácilmente.

Al final, Tavani expone el problema de la protección de la privacidad personal en el espacio público, es diferente que una persona este expuesta en un mercado y que las personas puedan ver los productos que compras o el momento en que lo haces, a comprar en línea, en donde todos los movimientos son registrados cuidadosamente, usando esa información para otros fines, en la que se viola la integridad contextual de la que hablaba Nissenbaum. Otras preocupaciones de la cibertecnología a la privacidad son los motores de búsqueda y la divulgación de esa información en dos diferentes prácticas, el registro de la información de cada búsqueda y el permitir a las personas adquirir información de cualquier otro con gran facilidad. Para poder darle una contra a estos problemas se han generado tecnologías para mejorar la privacidad, las PETS, herramientas que permite navegar por internet de forma anónima, sin embargo, estas poseen ciertas limitaciones por lo cual algunos defensores de privacidad exigen

legislaciones que regulen a la industria, con lo han hecho los países de la Unión Europea o Canadá.

La seguridad en el contexto de cibertecnología, no tiene un consenso que unifique el concepto. Para Epstein existen tres elementos claves, confidencialidad, que se refiere a evitar el acceso a la información a personas no autorizadas, integridad que es la prevención a los ataques que modifiquen la información y accesibilidad en la que la información sea accesible solamente a usuarios autorizados. En el desarrollo de este capítulo, seguridad en el ciberespacio, Tavani examina solo algunas formas de problemas de seguridad. La primera de ellas es la relación de la ciberseguridad con el ciberdelito, es importante recalcar, que las infracciones de ciberseguridad y el ciberdelito son consideradas como subcategorías de ciberética, sin embargo, no todos los delitos implican infracciones. Tavani pone tres ejemplos con respecto a este punto, el uso de una computadora para solicitar seño con infantes, traficar drogas y piratear música, aunque estas actividades sean ilegales, no significa inseguridad en las computadoras, es por eso que este tema de ciberdelito tiene distinciones en cuestiones de seguridad, por lo tanto, el capítulo actual, solo tendrá atención en las amenazas reales.

Existe una relación entre el capitulo anterior, sobre la privacidad, con respecto a la seguridad, algunos consideran el derecho a la privacidad con resultado de la seguridad, por ejemplo, la preocupación de la privacidad, se acaban cuando se asegura que la información almacenada en las bases de datos esta segura. Pero no todos están de acuerdo con este argumento, ya que como se vio en el capitulo 5, existen herramientas como las PETs que protegen al usuario en el ciberespacio dándole anonimato protegiéndole su derecho a privacidad, sin embargo, esto puede dificultar la identificación de violadores de seguridad. Tavani categoriza los problemas de ciberseguridad en 3, la seguridad en datos, el sistema de seguridad, y la seguridad de la red. La primera se refiere a la seguridad que reside en las bases de datos y como son tratos estos datos en donde se debe mantener una integridad de la información. En la actualidad la seguridad se ve amenazada por la computación en la nube, ya que usuarios no autorizados pueden acceder a la información. la segunda corresponde al

hardware y al SO, en esta categoría se encuentran los virus, gusanos informáticos y los malwares. la última enmarca temas de seguridad de infraestructura de la red, los ataques de seguridad a esta categoría van desde programas que interrumpen las actividades, hasta dejar prácticamente inoperable a internet.

Como se vio en la primera categoría, la computación en la nube amenaza la seguridad, en el entorno de seguridad de datos. Para contextualizar, Tavani hace referencia a la definición de computación en la nube de Knorr y Gruman, en donde la nube es cualquier recurso que se use externo al firewall, mientras que para el NIST (Instituto Nacional de estándares y Tecnología) es un modelo que habilita el acceso a la red, a un grupo de recursos informáticos. Para Cavoukian, este modelo genera al menos cuatro tipos de preocupaciones, la primera es como controlar sus datos almacenados, la segunda es la integridad, el acceso a los datos y por último es quien actualmente es el dueño de la información almacenada en la nube. Para David Talbot, genera otras preocupaciones como, la perdida accidental de datos, los ataques de piratería y el robo por empleados deshonestos.

Después de las amenazas en la nube, Tavani explica los conceptos de Hacking y ética del hacker, para Simpsons, un hacker es quien accede a un sistema informático, sin autorización, por otro lado, están los crackers, que tienen la intención de dañar y destruir datos. En el libro, Tavani explica que la referencia a los hackers en el capítulo 6 se hace a aquellos entusiastas de la informática sin causar daño a los sistemas. Al documentar estas personas, se usan expresiones de ética del hacker, que según Steven levy, basado en 6 principios, en los cuales hacen alusión sobre como abordar su oficio. Sin embargo, los mismos piratas informáticos han adoptado 3 principios, la información debe ser gratuita, los piratas brindan a la sociedad un servicio útil y las actividades realizadas en el ciberespacio no dañan a las personas en el mundo real. Todos estos desafíos, según Schneier se pueden entender analizando en términos de resultado entre diferentes elementos. Sin embargo, no esta claro quien tiene la responsabilidad moral, si las empresas privadas o el sector publico ya que este panorama se encuentra cada vez mas desperimetrizado.

References

Tavani, H. T. (2011). *Ethics and technology: Controversies, questions, and strategies for ethical computing*. John Wiley & Sons.