



XII Congreso ISKO España
II Congreso ISKO España-Portugal

**Organización del conocimiento:
sistemas de información abiertos**

ACTAS



International Society for Knowledge Organization
ISKO España – Portugal

II Congreso ISKO España-Portugal XII Congreso ISKO España

Organización del conocimiento:
sistemas de información abiertos

ACTAS

Murcia
Universidad de Murcia
2015

Ficha técnica:

Título: *Organización del conocimiento: sistemas de información abiertos*

Autor: II Congreso ISKO España y Portugal / XII Congreso ISKO España

Editores: José Vicente Rodríguez Muñoz, Isidoro Gil Leiva, Pedro Manuel Díaz Ortuño, Francisco Javier Martínez Méndez.

Edición: Facultad de Comunicación y Documentación. Universidad de Murcia.

ISBN: 978-84-608-3558-5

UNIVERSIDAD DE
MURCIA



ISKO – Ibérico 2015 Murcia

XII Congreso ISKO España / II Congreso ISKO España-Portugal Universidad de Murcia, 19 y 20 de noviembre de 2015.

Lema: Organización del conocimiento: Sistemas de información abiertos

Si aceptamos al conocimiento como el sujeto que trabaja para observar e interpretar la realidad de los objetos, esto es, los datos, podemos interpretar a la información como el elemento catalizador que permite alcanzar un nuevo orden, dicho de otro modo, como un proceso que transforma la incertidumbre en realidad, el caos en orden. En este contexto, para la sostenibilidad de cualquier sistema, entendido este en su expresión más amplia, se vislumbra como necesario que su estado sea el de un sistema abierto, de forma que permita el libre intercambio y por ende, una evolución sostenida.

Hitos

- Modelos de organización del conocimiento. Modelaje de sistemas y ciclo de vida de la información.
- Entornos y sistemas para la organización del conocimiento. Diseño, normalización e interoperabilidad de sistemas de información abiertos.
- Instrumentos para el acceso y transparencia de la información: gestión de documentos, plataformas digitales y archivos.
- Usuarios y usos de la información. Patrones vinculados a la transparencia y el gobierno abierto.
- Gobernanza y Auditoría de información en la organización del conocimiento.
- Representación del conocimiento: procesos y herramientas en sistemas abiertos y multilingües.
- Epistemología en la organización del conocimiento.
- Igualdad, género y diversidad en la organización del conocimiento.

Coordinadores Generales

- José Vicente Rodríguez Muñoz. *Universidad de Murcia.*
- Rosa San Segundo Manuel. *Universidad Carlos III de Madrid.*

Comité Organizador

- Isidoro Gil Leiva. *Universidad de Murcia.*
- Francisco Javier Martínez Méndez. *Universidad de Murcia.*
- Pedro Manuel Díaz Ortuño. *Universidad de Murcia.*
- José Antonio Gómez Hernández. *Universidad de Murcia.*
- José Antonio Frías Montoya. *Universidad de Salamanca.*
- Rosana López Carreño. *Universidad de Murcia.*
- Juan Antonio Pastor Sánchez. *Universidad de Murcia.*
- Tomás Saorín Pérez. *Universidad de Murcia.*

Comité Científico

- Emilia Currás Puente. *Miembro de Honor ISKO. España.*
- Adolfo Alonso Arroyo. *Universidad de Valencia.*
- María Luisa Alvite Díaz. *Universidad de León.*
- Virginia Bentes Pinto. *Universidade Federal do Ceará, Brasil.*
- María da Graça de Melo Simões. *Universidade de Coimbra, Portugal.*
- Carlos Cândido de Almeida. *Universidade Estadual Paulista, Brasil.*
- Dulce Amélia de Brito Neves. *Universidade Federal da Paraíba, Brasil.*
- Vera Lucia Doyle Louzada de Mattos Dodebei. *Universidade Federal do Estado do Rio de Janeiro, Brasil.*
- Ana Extremerño Placer. *Universidad de Alcalá.*
- José Pablo Gallo León. *Universidad de Murcia.*
- Jesús Gascón García. *Universitat de Barcelona.*
- Blanca Gil Urdicián. *Universidad Complutense de Madrid.*
- Ricardo César Gonçalves Santana. *Universidade Estadual Paulista, Brasil.*
- José Augusto Chaves Guimarães. *Universidade Estadual Paulista, Brasil.*
- Cristina Herrero Pascual. *Universidad de Murcia.*
- Manuela Moro Cabero. *Universidad de Salamanca.*
- José Antonio Moreira González. *Universidad Carlos III.*
- Luis Miguel Moreno Fernández. *Universidad de Murcia.*
- Antonio Paños Álvarez. *Universidad de Murcia.*
- Fernanda Peset Mancebo. *Universidad Politécnica de Valencia.*
- Antonio Pulgarín Guerrero. *Universidad de Extremadura.*
- Fernanda Antunes Ribeiro. *Universidade de Porto, Portugal.*
- Blanca Rodríguez Bravo. *Universidad de León.*
- Mariângela Spotti Lopes Fujita. *Universidade Estadual Paulista, Brasil.*
- Jualianne Texeira e Silva. *Universidade Federal da Paraíba, Brasil.*
- Jesús Tramullas Saz. *Universidad de Zaragoza.*
- Crispulo Travieso Rodríguez. *Universidad de Salamanca.*

Presentación

En primer lugar, felicitarnos todos por haber hecho posible una nueva edición de este Congreso y en particular a los todos los que han participado en la organización del mismo, sin cuyo esfuerzo no se hubiera hecho realidad. Todo ello, con una especial mención a los profesores, alumnos y personal de administración y servicios, por su intenso trabajo.

Y, debemos felicitarnos todos pues dado el contenido temático del congreso significa que nos va a permitir conocer la labor de numerosísimas personas que trabajan en el desarrollo de algo tan importante para el ser humano como son las Ciencias de la Información (bibliotecología, archivología, documentación y todo lo que comprende la gestión de la información y el conocimiento).

Siempre es importante que las personas se reúnan para compartir viejas, actuales y nuevas ideas, pues de seguro que de ese vínculo siempre se sale mejorado como científicos y como personas. Por ello, reivindico los tradicionales métodos epistolares en forma de comunicaciones, así como las exposiciones orales presenciales, nada sustituibles por la tecnología en su versión online. Nada que ver tanto en el modo del mensaje como en el modo de comunicación.

Lo que no quiero dejar de señalar es que además servirá para la exposición de ideas bajo diferentes puntos de vista, para el despliegue de nuevas ideas, para que todos, en definitiva, podamos compartir conocimiento.

Vamos a desarrollar el Congreso bajo el lema: “*Organización del conocimiento, sistemas de información abiertos*”. Puesto que ISKO es organización del conocimiento resulta ocioso señalar que en el actual devenir estamos en un continuo desarrollo de estructuras y artefactos que no sólo sean capaces de tener las capacidades de la legibilidad, sino que también tengan las de la inteligibilidad a modo de mimesis con el pensamiento humano, en la idea del manejo de grandes volúmenes de información y conocimiento que puedan ser usables.

La idea es que la meta de la Ciencia de la Información sea percibir y controlar el conocimiento en sus distintas representaciones. Hoy afrontamos el ciclo de vida de la información desde diversas perspectivas, tanto representacionales como tecnológicas. Y en este asunto, las Tecnologías de la Información y de la Comunicación han sido y están siendo causa y efecto de este fenómeno, como consecuencia de su naturaleza disruptiva.

Tampoco es menos cierto que en el desarrollo e incorporación de las Tecnologías de la Información y de la Comunicación existe un riesgo inherente sobre ellas, lo que podríamos llamar el lado oscuro de la globalización, y que no deja de ser un punto débil que amenaza el horizonte, esto es, el de crear mayores desigualdades entre los seres humanos, desigualdades que es denominada, no sin cierto eufemismo “brecha digital”.

Pero, a mi entender, no creo que resulte banal la segunda parte de ese lema, los sistemas abiertos. Quiero indicar con la idea de abiertos, no sólo la plétora de conceptos, procedimientos, técnicas, etc. que ellos implican y que en ellos están imbricados; entiéndase: software abierto, aplicaciones abiertas, metadatos, datos abiertos y/o enlazados; así como todo aquello que más o menos de forma colateral está relacionado, como, interoperabilidad, visibilidad, usabilidad, accesibilidad, transparencia, etc.

Lo que interesa es resaltar el concepto intrínseco que sostiene la idea de sistema abierto, frente a sistema asilado y cerrado. Frente a estos dos últimos, cuya cuyo final es predecible desde su nacimiento, esto es la muerte, los sistemas abiertos son la incertidumbre, pero la incertidumbre creativa, el caos determinista que ha permitido y permite entre otros fenómenos la biodiversidad.

Es en este extremo donde se manifiesta la importancia de la organización del conocimiento y los sistemas abiertos, pues sólo desde este enfoque, sólo desde esta ideología seremos capaces, ya no sólo de avanzar, sino de seguir creando. ¿Qué es sino la creatividad? La posibilidad de enriquecernos intelectualmente a través de entornos de incertidumbre.

El ser humano ha creado el concepto abstracto de dato como medio para establecer equilibrios con los objetos susceptibles de ser descritos, equilibrios que en los sistemas abiertos no son permanentes, lo que nos obliga a un continuo ajuste para adaptar los escenarios que queremos representar. Unas veces

los adaptamos, en otras no es posible, esto obliga a construir otros nuevos donde volver a un equilibrio, lo que sucede es que estos nuevos son tan diferentes a los iniciales que representan una nueva visión de la realidad. Y este es el gran papel del concepto de abierto.

Es por ello, que entendemos que la sustanciación de la organización del conocimiento y los sistemas abiertos no es vana, pues de ese modo no sólo incorporamos transparencia, elemento central en las sociedades modernas y exigencia incuestionable en la actualidad. Sino que, como tales sistemas abiertos, permitamos que su esencia, la evolución y la diversidad, se haga patente en la superación de las amenazas y debilidades actuales y generemos nuevas fortalezas y oportunidades para que el conocimiento humano sirva a sus fines. No apartemos del horizonte esta idea, integrémosla en todo aquello que nos incumba y no sólo me refiero en lo científico, sino en todas nuestras actividades.

Ahora procede que sean los congresistas los que tomen la palabra con las ideas y propuestas que han traído y que quedan expresadas en el presente documento. Espero y deseo que les sea de lo más gratificante y fructífero posible, que de seguro lo será.

Murcia, 19 de Noviembre de 2015

José Vicente Rodríguez Muñoz

TABLA DE CONTENIDO

Presentación.....	7
PONENCIA INAUGURAL	11
Perfis de Aplicação de Metadados: o quê, porquê, quando e como.....	12
Hito 1: Modelos de organización del conocimiento. Modelaje de sistemas y ciclo de vida de la información.....	15
O modelo científico no domínio de organização do conhecimento: um estudo a partir dos trabalhos apresentados nos congressos internacionais da ISKO	16
Catologação sob a perspectiva dos artigos publicados em revistas científicas nacionais avaliados nos estratos B1, B2 e B3 no sistema Qualis a partir de 1998.....	24
O profissional da informação na elaboração de políticas públicas de informação e tecnologia	37
A Informação Contábil na construção do conhecimento organizacional: uma modelagem a partir da DRE	41
Aplicação de reengenharia de tesouro: modelagem do THESAGRO	50
The Future of Knowledge Organization and Information Organization	61
HotWheels: catalogação e recuperação da informação em miniaturas de carros colecionáveis	67
Hito 2: Entornos y sistemas para la organización del conocimiento. Diseño, normalización e interoperabilidad de sistemas de información abiertos.	82
Bibliotecas eclesiásticas de Castilla y León. Visibilidad y acceso web	83
Modelagem de dados para representação descritiva no domínio da História da Arte: uma proposta para a construção de um banco de dados	96
OntoSmart: proposta de um modelo de recuperação de informação baseado em ontologia	105
Estudo da comunicabilidade da interface e do comportamento de busca da informação no Portal de Periódicos da CAPES	116
Elaboração de um vocabulário taxonómico sobre História Medieval portuguesa: problemas e desafios	130
Apropriação do Conhecimento na Web de Dados - Gestão de Recursos Computacionais em Sistemas Abertos ...	138
Organización del conocimiento en entornos wiki: una experiencia de organización de información sobre lecturas académicas	152
Sistema de informação aberto como recurso de organização do conhecimento e de mediação da aprendizagem..	160
Hito 3: Instrumentos para el acceso y transparencia de la información: gestión de documentos, plataformas digitales y archivos.....	172
A justiça na <i>web</i> : estudo sobre a gestão da informação em processos judiciais eletrónicos no Brasil.....	173
Abordagem sobre vocabulários controlados para arquivos: conceitos, aplicações e metodologias.....	187
Clasificación y indización de la información en Registros y Archivos de Gestión de las universidades	195
La búsqueda de información en herramientas de descubrimiento y OPAC's: fortalezas y debilidades.....	206
Gestão do Conhecimento nas Organizações de Ensino: recorrência de registros na <i>Web of Science</i>	220
Hito 4: Usuarios y usos de la información. Patrones vinculados a la transparencia y el gobierno abierto....	233
Competências infocomunicacionais para acesso e uso da informação.....	234
Hito 5: Gobernanza y Auditoría de información en la organización del conocimiento.	243
Uso de taxonomia sobre privacidade para identificação de atividades encontradas em termos de uso de redes sociais	244
Hito 6: Representación del conocimiento: procesos y herramientas en sistemas abiertos y multilingües ...	257
Aplicabilidad del mapa conceptual en la representación del conocimiento registrado en las historias clínicas del paciente.....	258
Armonización de ISO 25964 y SKOS en software de gestión de tesauros. Propuesta de análisis	266
Organização do conhecimento e tratamento da informação: analisando a subjetividade no processo de indexação e implicações na recuperação da informação.....	279
Metadatos en noticias: un análisis internacional para la representación de contenidos en periódicos.....	290
Perspectivas metodológicas para a representação da informação do documento de arquivo	304
Construção de macroestrutura de categorias de linguagem documentária em economia: proposta de inovação metodológica.....	319

Política de indexação para bibliotecas universitárias: um estudo com docentes da área de Organização e Representação do Conhecimento.....	332
Compatibilidade entre linguagens documentais para construção, atualização e adequação de vocabulário de bibliotecas universitárias.....	345
Organização e Representação do Conhecimento sobre Seca no Brasil: o caso do Núcleo Temático da Seca e do Semiárido da UFRN.....	357
Organização da Informação em Contexto Dinâmico e Sensível: Tesouro de Inteligência Policial.....	362
Terminología del huipil triqui	373
Representação de Contexto em Acervos Digitais.....	387
Aplicação da Teoria da Análise Facetada e Mapas Conceituais para navegação facetada em uma ontologia de domínio: resultados preliminares	398
Abordagens cognitivas da ciência da informação no Brasil: mapeamento conceitual	411
Organização da Informação no ambiente Web: produzindo conhecimento a partir de grandes volumes de dados ..	419
A representação da imagem do bibliotecário nas histórias em quadrinhos (HQs): um estudo descritivo	430
Estudo da Produção e Divulgação Científica do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo: Uso do software livre Script Lattes	438
Cognição, neuromarketing e neuroeconomia: entendendo as decisões dos atores baseados em informações	446
Organização do conhecimento arquivístico: um estudo terminológico comparativo (português, espanhol, francês, inglês) sobre classificação e descrição na <i>Multilingual Archival Terminology – ICA</i>	461
Políticas de indexación en bibliotecas escolares de Brasil y Portugal: análisis comparativo	470
Categorización de revistas científicas españolas en las bases de datos ISOC	485
Hito 7: Epistemología en la organización del conocimiento	497
Aportaciones Semióticas de la Documentación en España a la Organización Del Conocimiento: un análisis preliminar	498
Referentes Teóricos em Organização do Conhecimento: uma Análise de Domínio na ISKO Espanha (2005-2013).....	508
Referentes e interlocuções teóricas em análise documental no contexto brasileiro de Ciência da Informação.....	518
Exaustividade e especificidade na indexação: uma análise de conteúdo como perspectiva de investigação sobre o tema.....	527
La construcción de la Biblioteconomía como ciencia y su relación con la clasificación	533
A dimensão conceitual da organização do conhecimento no universo científico da ISKO: uma análise de domínio a partir dos congressos de ISKO-Brasil e ISKO- Espanha.....	544
Organização da informação e do conhecimento no contexto da Ciência da informação: da análise terminológica à reflexão epistemológica	556
Referentes teóricos basilares na ISKO-Ibérico e suas contribuições para a Organização do Conhecimento (OC)..	570
Organização e representação da informação em arquivos: uma análise a partir da função classificação.....	579
O “nome próprio” no contexto da Epistemologia da Organização do Conhecimento: um debate filosófico-teórico ..	584
Hito 8: Igualdad, género y diversidad en la organización del conocimiento	597
Sesgo y universalidad: un enfoque histórico-conceptual	598
Interações entre Semiótica da Cultura e Organização do Conhecimento: conceitos integradores.....	603
Información y crianza con apego en España	618
Formação discursiva, sistemas de classificação e o discurso estrangulado de Charlie Hebdo: impactos, desdobramentos e implicações na representação da informação da ciência da religião no século XXI.....	629
Presentación comercial.....	636
TesaurVAL: software para la creación y gestión de tesauros	637
Índice de autores.....	638

Hito 1: Modelos de organización del conocimiento. Modelaje de sistemas y ciclo de vida de la información

Hito 2: Entornos y sistemas para la organización del conocimiento. Diseño, normalización e interoperabilidad de sistemas de información abiertos.

Hito 3: Instrumentos para el acceso y transparencia de la información: gestión de documentos, plataformas digitales y archivos

Hito 4: Usuarios y usos de la información. Patrones vinculados a la transparencia y el gobierno abierto

Hito 5: Gobernanza y Auditoría de información en la organización del conocimiento.

Hito 6: Representación del conocimiento: procesos y herramientas en sistemas abiertos y multilingües

Hito 7: Epistemología en la organización del conocimiento

Hito 8: Igualdad, género y diversidad en la organización del conocimiento

Uso de taxonomia sobre privacidade para identificação de atividades encontradas em termos de uso de redes sociais

Using Privacy's Taxonomy to identify activities found on Social Network's terms of use

Fernando de Assis Rodrigues, M.S. (1), Ricardo César Gonçalves Sant'Ana, Dr. (2)

(1) Universidade Estadual Paulista, Programa de Pós-Graduação em Ciência da Informação, avenida Hygino Muzzi Filho, 737 – Marília, Brasil – 17.525-000, fernando@elleth.org

(2) Universidade Estadual Paulista, Departamento de Ciência da Informação, avenida Hygino Muzzi Filho, 737 – Marília, Brasil – 17.525-000, ricardosantana@marilia.unesp.br

Resumo

O objetivo deste trabalho é explicitar, a partir dos termos de uso de redes sociais, elementos que permitam identificar possíveis atividades que apresentem efeitos potencialmente prejudiciais a privacidade, seja por agentes internos ou externos. Para tanto, utilizou-se a Taxonomia da Privacidade de Solove para estabelecer uma categorização destas ações nos termos de uso disponibilizados pelas redes sociais, com enfoque nas diretrizes estabelecidas nestes termos sobre questões inerentes as fases de coleta e armazenamento de dados pessoais. O universo de pesquisa foi delimitado ao estudo dos termos de uso de três das principais redes sociais no momento da pesquisa. Os resultados estão divididos em duas partes: a primeira, identifica indícios de possíveis atividades prejudiciais à privacidade, através da vinculação das características de trechos nos termos de uso com os conceitos da taxonomia, e; a segunda, apresenta comparações entre as classificações possibilitadas pela taxonomia e seu nível de ocorrência nos termos de uso estudados. Concluiu-se que a aplicação de uma taxonomia apropriada pode auxiliar no estudo de termos de uso, possibilitando a explicitação de atividades previstas nestes termos, o que permite inclusive, propostas de futuras aplicações desta metodologia em outros contextos.

Palavras-chave: Privacidade. Tecnologias da Informação e Comunicação. Dados pessoais. Redes Sociais. Taxonomia da Privacidade.

Abstract

The aim of this study is to explicit elements on social networks who allow the identification of possible activities that shows harmful effects on privacy, either when executed by internal or external agents. To achieve that, this work uses the Privacy Taxonomy by Solove to categorize those potentially harmful actions found on social network's terms of use, specially to emerge aspects inherent in data gathering and data storing phases using personal data. The universe of study was delimited to study terms of use from three prominent social networks at the time of the research. The results are divided into two parts: the first tries to identify evidences of possible activities harmful to privacy, through a linkage of characteristics in terms of use with concepts from Privacy Taxonomy. The second shows a comparison between classifications (enabled when the taxonomy was applied), and occurrences levels of this kind of activities on terms of use. It was concluded that applying an appropriated taxonomy can help on terms of use studies, enabling to explicit predicted activities in those terms of use, which allow, indeed, proposals of new applications of this methodology in others digital contexts.

Keywords: Privacy. Information and Communication Technologies. Personal data. Social Networks. Privacy Taxonomy.

1. Introdução

A penetração de Tecnologias da Informação e Comunicação (TIC) nas ações e atividades humanas – centradas em uma sociedade em rede, em que o principal ativo é a informação (Castells, 2003) – possibilitou o estabelecimento de um sistema que suportasse a formação de redes com milhares de usuários conectados, com a finalidade de troca de informações sobre inúmeros temas, além de representar um novo

local de organização social e cultural (Castells, 2002).

A internet oferece uma infraestrutura que permite o fluxo de inúmeros tipos de dados e documentos e com a criação em 1989 do protocolo *HyperText Markup Language (HTML)*, surgiram plataformas com o intuito de fornecer suporte às redes de informações e inter-relacionamento entre pessoas, denominadas redes sociais on-

line ou redes sociais (1) (Adamic e Adar, 2003; CERN, 2015).

As redes sociais estão presentes desde o início da internet (Adamic e Adar, 2003), e com o amadurecimento das tecnologias envolvidas neste cenário, estas redes sociais oferecem serviços específicos para o inter-relacionamento de seus usuários e para a troca de informações em formato multimídia, como imagens, vídeos, áudios, hiperlinks, e textos (Mislove, et al., 2007).

Algumas das redes sociais em atividade na década de 2010 atingiram números expressivos quando relacionados a população mundial (2). No mês de dezembro de 2014, a rede social Facebook (3) possuía uma média de 1,19 bilhão de usuários mensais e ativos. Portanto seus usuários representavam, aproximadamente, 17% da população mundial. Outras redes sociais apresentavam números totais acima de 250 milhões de usuários ativos, tais como o Instagram (4) e o Twitter (5) (BBC, 2014; Facebook, 2015a; WORLDOMETERS, 2015).

Para Mislove et al. (2007), os sítios destas redes sociais são parte integrante do conjunto dos serviços mais acessados e utilizados da internet.

As redes que são elaboradas e mantidas por instituições e empresas privadas para a troca de informações e experiências pessoais suscitam preocupações já existentes em outros contextos como: exposição de dados sensíveis de usuários para empresas, governos e, inclusive, para outros usuários; a perseguição de pessoas; ações resultantes de intolerância; entre outros. Em todos estes cenários, ocorrem exposições que perpassam questões inerentes a privacidade (Fogel e Nehmad, 2008; Krasnova, et al., 2009; Young e Quan-Haase, 2009; Chen e Zhao, 2012).

Destaca-se ainda que problemas relacionados a privacidade de usuários em redes sociais não são causadas somente pelo uso de TIC (que pode fazer papel de agente catalisador na coleta automatizada de grandes quantidades de dados sobre usuários), mas também pela atividade de usuários, de agentes externos e de controladores que possuam conhecimento suficiente para coletar e processar estes dados com outras fontes, estabelecendo novos dados potencialmente prejudiciais à privacidade (Solove, 2006; Fogel e Nehmad, 2008).

Nesse contexto destacam-se duas dimensões da privacidade a serem estudadas: os resultados de interações entre redes e usuários na fase de coleta de dados, e; a delimitação sobre

o que é realizado com os dados sobre usuários, na fase de armazenamento. Ambas dimensões são efeitos do uso de TIC (Sant'Ana, 2013).

Todavia, generalizar atividades que são prejudiciais à privacidade dos usuários pelos detentores da informação contida nas redes sociais é tema complexo, pois usuários são informados e devem conceder aceitação aos termos de uso da rede social na etapa que realizam o cadastro de uma conta para acessar o serviço. Os termos de uso destas redes têm duplo papel neste processo: pacificador, enquanto elemento de percepção de segurança aos usuários, ao estabelecer limites e garantias legais sobre o que é realizado com dados pessoais, e; como elemento de opacidade entre usuários e os serviços sobre o uso de seus dados, diluído em uma alta complexidade da rede e no volume e variedade de ações e atividades passíveis de realização (Castells, 2002). Desta forma, os ambientes não oferecem condições mínimas de uma plena compreensão ou acompanhamento de potenciais ações (e seus efeitos ou impactos) prejudiciais sobre sua privacidade.

A partir desta complexidade sobre questões de privacidade, Solove (2006) propõe uma taxonomia voltada à dificuldade de segregar tipos de atividades existentes que incidem sobre a privacidade, denominada Taxonomia da Privacidade. Esta taxonomia tem como objetivo simplificar o entendimento das atividades que de alguma forma possam prejudicar ou violar a privacidade dos sujeitos; e está dividida em grupos. Cada grupo possui uma definição de sua atividade prejudicial, descreve o *modus operandi*, as características da violação e prejuízos causados.

2. Objetivos e procedimentos

Este trabalho tem como objetivo explicitar, a partir dos termos de uso de redes sociais, elementos que permitam identificar possíveis atividades que apresentem efeitos potencialmente prejudiciais a privacidade, seja por agentes internos ou externos. Para tanto, utilizou-se a Taxonomia da Privacidade, proposta por Solove (2006), para estabelecer uma categorização destas ações nos termos de uso (6) disponibilizados pelas redes sociais, com enfoque nas diretrizes estabelecidas nestes termos sobre questões inerentes as fases de coleta e armazenamento de dados pessoais.

O universo de pesquisa foi delimitado ao estudo das coleções de documentos que compõem os termos de uso das redes sociais: Facebook, Instagram e Twitter. Esta escolha levou em consideração a quantidade de usuários ativos des-

tas redes, apresentada na introdução deste texto.

Não é escopo deste trabalho a análise se estes termos de uso garantem ou não a privacidade de dados pessoais para uma determinada atividade; mas sim, restringe-se a identificar, por meio de uma taxonomia apropriada, possíveis atividades potencialmente prejudiciais à privacidade de seus usuários. Também não é parte integrante as delimitações de localização (externa ou interna ao serviço) do potencial agente de execução destas atividades.

Como metodologia foi traçada uma análise sistematizada, a partir da leitura das coleções de documentos que compõem cada termo de uso das redes sociais, divididas em 3 etapas.

A primeira etapa (segundo capítulo) consiste na explicitação dos grupos de atividades prejudiciais à privacidade, a partir da proposta de categorização apresentada na Taxonomia da Privacidade de Solove (2006).

A segunda, identifica características nos termos de uso sobre questões de dados pessoais de seus usuários, a partir do isolamento de seções e de trechos identificados nos documentos disponíveis, apresentados no terceiro capítulo.

A terceira etapa – quarto capítulo – apresenta os resultados da correlação entre os subgrupos da Taxonomia da Privacidade e as características identificadas nos termos de uso, e estão divididos em duas partes: a primeira, identifica indícios de possíveis atividades prejudiciais à privacidade, através da vinculação das características de trechos nos termos de uso com os conceitos da taxonomia, e; a segunda, apresenta comparações entre as classificações possibilitadas pela taxonomia e seu nível de ocorrência nos termos de uso estudados.

3. Estrutura da Taxonomia da Privacidade

A Taxonomia da Privacidade (7) é composta por quatro grupos: Coleta de Informação, Processamento de Informação, Disseminação de Informação e Invasão, que neste trabalho passamos a identificar como Grupo I, II, III e IV, respectivamente.

Os grupos estão divididos em subgrupos, conforme o Quadro I (Anexo 1), que a síntese da taxonomia, agrupando conceitos das atividades prejudiciais à privacidade, relacionando-as com seus respectivos subgrupos.

Grupo I: Coleta de Informação

O primeiro grupo, denominado Coleta de Informação, envolve atividades de violação de privacidade no momento da coleta de dados sobre um indivíduo ou um coletivo de indivíduos. Este grupo está dividido em dois subgrupos: Vigilância e Interrogatório.

O subgrupo Vigilância concentra atividades encadeadas com o propósito de vigiar um indivíduo no seu espaço privado ou em espaço público.

Por exemplo, um serviço disponível na internet pode processar dados coletados em diferentes momentos sobre um usuário, sob a justificativa de uso destes na melhoria da experiência do usuário em sua plataforma; e executar ações de vigilância como o direcionamento de conteúdo a partir de dados coletados sobre trajetos do usuário (incluindo as coordenadas geográficas, a umidade, a pressão atmosférica e a altitude); informações do dispositivo de acesso e da rede de dados; histórico de comandos por voz; gostos e experiências sobre locais visitados; tempo de permanência em um local público ou privado; informações sobre a conexão de rede; metadados de imagens, áudios e vídeos; entre outros.

O subgrupo Interrogatório concentra atividades de processos de coleta de dados, baseados em interrogatórios e entrevistas.

Um exemplo são sítios que possuem, no processo de ingresso, formulários com campos de preenchimento obrigatório contendo informações que podem ser sensíveis para certa audiência – e caso o usuário não possua o interesse em compartilhar tais informações, não terá acesso ao serviço.

Grupo II: Processamento de Informação

O segundo grupo é denominado Processamento de Informação. Este grupo envolve atividades prejudiciais à privacidade a partir do processo de armazenamento (de persistência), de manipulação e de uso de dados sobre indivíduos. Este grupo está dividido em cinco subgrupos: Agregação, Identificação, Insegurança, Uso Secundário e Exclusão.

O subgrupo Agregação está ligado a atividades vinculadas ao processo de combinação de dados de múltiplas fontes sobre indivíduos, com o propósito de revelar fatos ocultos, quando eram analisados de forma separada.

Por exemplo, um usuário de uma rede social pode fornecer dados sobre sua relação matrimonial (ao preencher informações do seu perfil) e, em outro momento, navegar na internet por páginas sobre locais para o turismo voltado à celebração de lua de mel. Um agente externo,

que possuir o acesso para coletar estes dados, pode inferir, através de algoritmos especializados em agregação de dados, se este indivíduo tem propensão ou não para futuramente comprar produtos e serviços para recém-casados. Ao combinar dados destas fontes, o agente externo realiza uma atividade do subgrupo Agregação.

O subgrupo Identificação consiste em atividades a partir do processo de vinculação de dados que permitam a (re)identificação de usuários (e de seus dados pessoais) com suas respectivas pessoas.

Serviços na internet que oferecem acesso a dados sobre seus usuários podem ser passíveis de coleta destes conjuntos de dados por agentes externos – e estes podem ter a *expertise* necessária para recombinar estes conjuntos de dados coletados com outros dados (de outras plataformas), aumentando o repertório de informações sobre um determinado usuário e (re)identificando-o em diversos domínios (até vinculando estes dados com documentos pessoais, como números de seguro social ou cartão de crédito). Este tipo de atividade é parte integrante do subgrupo Identificação.

O subgrupo Insegurança compreende atividades que não garantem segurança sobre questões de acesso a dados pessoais aos envolvidos.

Por exemplo, quando uma rede é alvo de uma coleta de dados externa não autorizada, através de técnicas como o *exploit*, o resultado é um vazamento de dados pessoais que não há possibilidade de retorno ao estágio anterior (quando não havia o vazamento). Ou seja, como a política de acesso a estes dados foi comprometida e não há mais garantias que não existam cópias destes dados sob tutela de terceiros – uma atividade ligada ao subgrupo Insegurança.

No subgrupo Uso Secundário estão contidas atividades que envolvem o uso de dados coletados para um determinado propósito e utilizados *a posteriori* para outras finalidades.

Quando dados são coletados sobre indivíduos com um propósito e são utilizados para outra finalidade, sem consentimento, tais como o uso e compartilhamento de dados pessoais a terceiros para personalização de propagandas, são atividades que integram o subgrupo Uso Secundário.

O subgrupo Exclusão consiste nas atividades que apresentam opacidade ao indivíduo nos processos: de armazenamento de dados pessoais; no compartilhamento destes dados a terceiros, e; na ausência ou na inabilidade de

participação nas decisões sobre questões envolvendo a coleta, o armazenamento, o uso e o compartilhamento destes dados.

Por exemplo, uma rede social em que o indivíduo desconhece, não tem acesso ou não participa de decisões sobre o uso de seus dados, é uma atividade integrante do subgrupo Exclusão.

Grupo III: Disseminação de Informação

O terceiro grupo é denominado Disseminação de Informação e envolve atividades de publicação, exposição e disseminação de informações sobre indivíduos. Está dividido em sete subgrupos: Quebra de Sigilo, Divulgação, Exposição, Aumento do Acesso, Chantagem, Apropriação e Distorção.

O subgrupo Quebra de Sigilo consiste em atividades em que ocorrem a quebra de confiança entre as partes em manter a confidencialidade das informações sobre indivíduos.

Um serviço que estabelece em seus termos de uso o não-compartilhamento de dados pessoais a terceiros e, *a posteriori*, estes dados estão disponíveis para um público externo pré-selecionado ou são acessíveis de forma direta ou indireta publicamente, desenvolve-se uma atividade integrante do subgrupo Quebra de Sigilo.

O subgrupo Divulgação consiste em atividades de divulgação e de disseminação de informações sobre um indivíduo, que acarretam mudanças na maneira que outros indivíduos julgam seu caráter.

Quando não está transparente a usuários qual o repertório de informações estará disponível para seus pares e para as conexões de seus pares, este tipo de atividade ofusca a real delimitação da possível audiência, o que pode acarretar um julgamento sobre seu caráter sobre questões de cunho privado a partir de dados pessoais. Este tipo de atividade é parte do subgrupo Divulgação.

O subgrupo Exposição consiste nas atividades vinculadas a exposição para terceiros de atributos emocionais ou físicos de intimidade do indivíduo, tais como a nudez, funções corporais e informações de cunho privado.

Sítios de compartilhamento de conteúdos multimídia podem armazenar e preservar (persistir) dados sobre fotografias e vídeos pessoais sem o consentimento ou pleno entendimento dos envolvidos, revelando sua intimidade a terceiros. Mesmo que o conteúdo possa ser removido a intimidade dos envolvidos já foi revelada, parte de uma atividade do subgrupo Exposição.

O subgrupo Aumento do Acesso agrupa atividades que visam amplificar o acesso a dados pessoais além do previsto ou do combinado entre as partes.

Quando um sítio compartilha dados de usuários com outros serviços (próprios ou de terceiros) amplia o acesso a estes dados além do previamente consentido, mesmo quando este processo está explicitado no termo de uso, pois dados pessoais enviados a estes serviços estão mais sujeitos aos seus respectivos termos de uso, mas sim aos termos de uso dos outros serviços – e estes outros serviços podem ter, em seus termos de uso, delimitações distintas sobre quais dados pessoais serão (re)compartilhados com seus parceiros. Esta atividade é parte do subgrupo Aumento do Acesso;

O subgrupo Chantagem agrupa atividades de controle, de dominação, de intimidação ou de ameaças a pessoas ou grupos, por terceiros.

A ocorrência de chantagens, intimidações e ameaças de grupos ou de indivíduos, com o uso da extorsão para angariar recursos financeiros a partir da revelação de dados pessoais (como fotografias íntimas), integra o subgrupo Chantagem.

No subgrupo Apropriação estão concentradas atividades que utilizam dados pessoais de um determinado sujeito em benefício de um terceiro ou para cancelar um serviço ou um produto, sem o pleno consentimento do sujeito.

Uma rede que utiliza de dados pessoais e fotos de seus integrantes para cancelar produtos de seus colaboradores executa uma atividade integrante do subgrupo Apropriação.

O subgrupo Distorção compreende atividades de disseminação de informações falsas ou interpretadas de maneira dúbia sobre um indivíduo.

Sítios que divulgam parte dos dados pessoais em um catálogo público, a partir da coleta de dados sobre usuários de outras redes sociais, podem descontextualizar estas informações, criando novas interpretações. É uma atividade do subgrupo Distorção.

Grupo IV: Invasão

O quarto grupo é denominado Invasão e engloba atividades de invasão à privacidade de indivíduos. O grupo está dividido em dois subgrupos: Intromissão e Interferência Decisional.

O subgrupo Intromissão consiste em atividades com o propósito de realizar incursões em assuntos ou em informações de caráter privado.

Por exemplo, a obrigatoriedade de instalar ferramentas ou utilizar serviços com propósito de gravar dados sobre ações em um determinado ambiente, sem consentimento das partes, é uma atividade do subgrupo Intromissão.

O subgrupo Interferência Decisional consiste em atividades de envolvimento do Estado em assuntos de caráter privado, executando decisões em nome do indivíduo.

Quando o Estado decide sobre ações de cunho privado, como partes do corpo humano ou sobre a privacidade dos indivíduos, estas atividades são parte integrante do grupo Interferência Decisional.

4. Características dos Termos de Uso

As redes sociais Facebook, Instagram e Twitter possuem, nos rodapés de seus respectivos sítios, uma área específica para o acesso aos termos de uso dos serviços oferecidos, com o rótulo intitulado *Terms* ou seu equivalente em língua estrangeira (8), e são explicitadas suas características, individualmente, nas seções a seguir.

4.1. Facebook

O termo de uso é composto por um documento principal denominado *Statement of Rights and Responsibilities* e onze documentos adicionais sobre serviços ou temáticas específicas que a rede social tem envolvimento direto ou indireto: *Data Policy*, com informações sobre a política sobre dados pessoais; *Payment Terms*, com termos adicionais sobre pagamentos pela ferramenta; *Platform Page*, com informações sobre intercâmbio de dados com aplicativos externos; *Facebook Platform Policies*, com as diretrizes para aplicações; *Advertising Guidelines*, com as diretrizes sobre publicidade na rede social; *Self-Serve Ad Terms*, com as diretrizes sobre publicidade para ferramentas conectadas a rede social; *Promotions Guidelines*, com as diretrizes para a elaboração de concursos e premiações; *Facebook Brand Resources*, com as diretrizes para utilização de material de propriedade do Facebook (copyright); *How to Report Claims of Intellectual Property Infringement*, com as diretrizes de direitos autorais; *Pages Terms*, com as diretrizes de uso para criação de páginas, e; *Community Standards*, contendo informações normas de boas condutas e ações aprovadas ou não sobre convivência entre seus usuários. Todos estes documentos estão disponíveis mesmo quando usuário não está identificado na rede social (Facebook, 2015b).

Segundo os documentos disponíveis, o usuário do Facebook, ao postar fotos e vídeos na plata-

forma, garante o direito compartilhado ao Facebook de utilização e transferência de seus dados pessoais a parceiros, em qualquer localidade e a qualquer momento, cessando quando o usuário exclui a sua conta. No documento *Data Policy*, está descrito que a plataforma pode compartilhar dados de usuários com outras empresas parceiras, tais como equipes de vendas externas, empresas de publicidade, escritórios regionais, entre outros (Facebook, 2015c).

O termo de uso não contém informações detalhadas sobre a forma que é realizado o processo de exclusão de dados pessoais a pedido do usuário. Todavia, é presente no texto que dados pessoais que forem relacionados à conteúdos licenciados com *copyright* ou compartilhados a terceiros podem continuar disponíveis, mesmo quando solicitado a sua exclusão (Facebook, 2015b).

Na quarta seção denominada *Registration and Account Security*, do documento *Statement of Rights and Responsibilities*, estão estabelecidas quais condutas são permitidas aos usuários, destacando-se que usuários da rede social devem concordar com a obrigação de informar todos os seus dados pessoais de forma “precisa e atualizada” (Facebook, 2015b, p. 1). A rede social reserva-se no direito de bloquear o acesso do usuário, caso considere que estes dados pessoais ou atividades exercidas na plataforma não estejam de acordo com as condutas preestabelecidas (Facebook, 2015b).

A décima sétima seção (denominada *Definitions*) do documento *Statement of Rights and Responsibilities*, contém a definição com o significado de alguns termos, como a definição para o termo plataforma, que denomina o conjunto de todos os serviços e Interfaces para Programação de Aplicativos externos (API, acrônimo proveniente do termo na língua inglesa) oferecidas pela empresa Facebook (Facebook, 2015b). Estas plataformas habilitam o compartilhamento de dados pessoais do Facebook por “[...] outros, incluindo desenvolvedores de aplicativos e administradores de sítios [...]” (Facebook, 2015b, p. 1).

No documento *Data Policy* é delimitado que metadados identificados nos conteúdos multimídias enviados por usuários são armazenados, como: a localização geoespacial, a data de criação do conteúdo, informações do dispositivo de acesso e do provedor de internet, o endereço IP, o idioma, protocolos, o número do telefone, entre outros (Facebook, 2015c).

O documento *Data Policy* explicita que informações sobre o usuário podem ser utilizadas na personalização de propagandas e em “[...] sis-

temas de medições para [...] exibir anúncios relevantes ou não dos nossos serviços e medir a efetividade e o alcance de nossos anúncios e serviços” (Facebook, 2015c, p. 1).

4.2. Instagram

O termo de uso está dividido em cinco documentos: *Terms of Use*, com informações gerais sobre o termo de uso; *Privacy Policy* com informações vinculadas a política de privacidade adotada pela rede social; *API Terms of Use*, com informações sobre os direitos e deveres de aplicações externas, que utilizam dados de seus usuários coletados através de API; *Community Guidelines*, contendo informações sobre atitudes aprovadas ou não de convivência entre seus usuários, e; *Intellectual Property*, com informações sobre *copyright* e licenciamentos (Instagram, 2015a). Todos estes documentos estão disponíveis mesmo para quando o usuário não está identificado formalmente na rede social.

Segundo os documentos disponíveis, o usuário do Instagram, ao postar fotos e vídeos na plataforma, garante o direito compartilhado ao Instagram de utilização e transferência de seus dados pessoais aos seus parceiros, em qualquer localidade e momento, cessando este direito quando o usuário exclui sua conta. No documento *Terms of Use*, para o usuário ter acesso aos aplicativos desenvolvidos por terceiros em sua conta, consentirá, *a priori*, a publicação de dados pessoais com a empresa terceirizada, como: o nome da conta, o nome de usuário e a foto do perfil (Instagram, 2015a).

O termo de uso não contém informações detalhadas sobre a forma que é realizado o processo de exclusão de dados pessoais a pedido do usuário. Todavia, é presente no texto que os dados pessoais que são compartilhados aos seus parceiros podem continuar disponíveis, sem informar um processo que possibilite a exclusão destes (Instagram, 2015a).

No documento *Terms of Use*, os itens 4, 5 e 6 da seção *General Conditions* definem que o sítio pode: bloquear o acesso, excluir ou forçar a modificação conteúdos ou nome de usuário, e; monitorar atividades de seus usuários a qualquer momento, sem aviso prévio (Instagram, 2015a).

No documento *API Terms of Use* é delimitado que o desenvolvedor de um aplicativo externo deve informar aos usuários como dados pessoais são coletados, armazenados, processados e disseminados (Instagram, 2015b).

O documento *Privacy Policy* informa ao usuário que metadados identificados nos conteúdos multimídias enviados por usuários são armazenados, como: a localização geoespacial, a data de criação, informações do dispositivo de acesso e do provedor de internet, o endereço IP, o idioma, protocolos, o número de telefone, entre outros (Instagram, 2015c).

4.3. Twitter

O termo de uso é composto por um documento principal denominado *Twitter Terms of Service* e cinco documentos adicionais sobre serviços ou temáticas específicas que a rede social tem envolvimento direto ou indireto: *The Twitter Rules*, com os princípios de convivência e uso da ferramenta; *Twitter Privacy Policy*, com informações sobre coleta, uso e compartilhamento de dados pessoais; *Developer Agreement & Policy*, com os direitos e deveres de parceiros desenvolvedores de aplicações externas, que utilizam dados de seus usuários; *Twitter Commerce Terms*, com termos adicionais sobre pagamentos e promoções pela ferramenta, e; *Inactive Account Policy*, com informações sobre exclusão ou a queda por desuso (9) de contas de usuários (Twitter, 2015a). Todos estes documentos estão disponíveis mesmo para quando o usuário não está identificado formalmente na rede social.

O documento do termo de uso principal da rede social estabelece, na seção *Privacy*, que todas as questões relativas ao uso de informações pessoais pelo sítio ou por terceiros são balizadas pelo documento auxiliar *Twitter Privacy Policy* (Twitter, 2015a, 2015b).

O usuário ao postar fotos e vídeos na plataforma garante o direito ao Twitter de utilizar e transferir a terceiros estas informações, em qualquer localidade e momento, salvo quando o usuário exclui o conteúdo. Também reserva-se no direito de compartilhar dados pessoais como: a localização geoespacial, a data de criação de conteúdos, textos, imagens, hiperlinks e o idioma com empresas parceiras e agências de publicidade, através de sua API (Twitter, 2015b).

Por padrão, as postagens de conteúdo do usuário é acessível de forma pública (Twitter, 2015b) e estes conteúdos associados aos dados pessoais sobre o usuário podem ser utilizados para personalizar propagandas e para o entendimento do público e o desenvolvimento do próprio serviço (Twitter, 2015a, 2015b).

5. Resultados

A primeira parte dos resultados apresenta os vínculos de indícios de possíveis atividades prejudiciais à privacidade com as características de trechos nos termos de uso com os conceitos da Taxonomia da Privacidade (Solove, 2006), agrupados por rede social. A segunda parte apresenta comparações entre as classificações possibilitadas pela taxonomia e seu nível de ocorrência nos termos de uso estudados.

5.1. Vinculação entre a Taxonomia da Privacidade e características dos termos de uso

Nesta seção, cada parágrafo apresenta características identificadas em trechos nos termos de uso e a vinculação com atividades dos subgrupos da Taxonomia da Privacidade são apresentados no final das sentenças. Um trecho pode ser vinculado com um ou mais subgrupos e subgrupos podem ser vinculados com ou mais trechos.

Facebook

Na rede social Facebook, o usuário não encontra um local ou documento que estabeleça quais são as empresas parceiras que acessam seus dados pessoais, sendo possível vincular este tipo de atividade ao subgrupo Aumento do Acesso.

Não é possível delimitar de forma transparente quais informações são geradas por empresas parceiras a partir de dados de usuários ou a forma que manipulam e processam estes dados pessoais com outras fontes de dados, o que pode acarretar atividades ligadas aos subgrupos Uso Secundário e Agregação.

Apesar do documento principal do termo de uso estabelecer em sua segunda seção, denominada *Sharing Your Content and Information*, que todos os dados sobre o usuário é de posse do mesmo (Facebook, 2015b), há certa opacidade no *modus operandi* por empresas parceiras após ter o acesso concedido aos dados pessoais, podendo ser um ambiente catalisador de possíveis atividades de quebra de sigilo, como estabelecido no subgrupo Quebra de Sigilo.

Segundo o *Data Policy* (Facebook, 2015c), conteúdos e dados pessoais podem ser compartilhados com empresas de publicidade. Estas empresas de publicidade estão aptas a utilizar dados pessoais (como gostos ou interesses do usuário por páginas, produtos ou serviços) para cancelar ofertas de produtos ou serviços perante o público da rede social, sem a devida transparência ao usuário sobre como este processo é realizado (como, por exemplo, determi-

nar qual foi o público ou o tempo de vigência desta ação), concomitante com atividades ligadas ao subgrupo Apropriação.

Apesar do termo de uso delimitar quais são as atividades permitidas aos usuários na rede social, há opacidade nos procedimentos sobre a arbitragem de supostas violações (como no caso do bloqueio de contas de usuário), diretamente ligado a questões inerentes aos subgrupos Exclusão, Vigilância e Insegurança.

O processo de exclusão de dados pessoais não é transparente ao usuário, principalmente no compartilhamento de conteúdo com seus pares e no vínculo de dados e gostos aos conteúdos *copyright*. Isto cria certa insegurança ao usuário sobre seu modo de agir na rede – já que não há garantias se o conteúdo publicado será excluído por completo, caso o usuário manifeste interesse – vinculando esta atividade ao subgrupo Insegurança.

É possível realizar a coleta de dados através da API, permitindo que possam existir ocorrências de ações de coleta automatizada, por agentes externos ao sítio, sem o consentimento prévio do usuário (pois são permissivos novos acordos com empresas parceiras, ao longo do tempo), podendo desencadear atividades vinculadas ao subgrupo Quebra de Sigilo.

A rede social Facebook pode compartilhar a foto, o nome e outras informações variáveis (não informadas) sobre usuários com empresas parceiras – e estas empresas podem agregar estes dados com suas bases de dados – permitindo que possam existir ocorrências de atividades vinculadas aos grupos: Agregação e Apropriação.

Não é transparente ao usuário se a rede social compartilha metadados dos conteúdos multimídia de usuários com empresas parceiras. Caso estes metadados sejam compartilhados, é possível agregá-los com dados pessoais, garantindo a estas empresas parceiras informações adicionais, como: a localização geoespacial e temporal do conteúdo, atividade que é parte do subgrupo Agregação.

Empresas de publicidade, parceiras da rede social, podem processar dados de usuários com outras fontes, com objetivo de personalizar propagandas e conteúdos a serem apresentados ao usuário. Também é permitindo estender o acesso a estas informações para terceiros, através da compra de espaços publicitários. Estas atividades estão ligadas aos subgrupos Uso Secundário e Agregação.

Como anúncios publicitários personalizados precisam, *a priori*, consumir dados pessoais

para aferir sua precisão, a empresa terceira necessita de acesso identificável sobre dados de cada usuário, permitindo a sua identificação sobre o grupo. Esta atividade é vinculada ao subgrupo Identificação.

Instagram

Na rede social Instagram, o usuário não encontra um local ou documento que estabeleça quais são as empresas parceiras que acessam seus dados pessoais, sendo possível vincular este tipo de atividade ao subgrupo Aumento do Acesso.

Não é possível delimitar de forma transparente quais informações são geradas por empresas parceiras a partir de dados de usuários ou a forma que manipulam e processam estes dados pessoais com outras fontes de dados, o que pode acarretar atividades ligadas aos subgrupos Uso Secundário e Agregação.

Não há transparência no processo de exclusão de dados pessoais, pois, mesmo com local apropriado para o pedido de exclusão de todos os dados pessoais da ferramenta pelo usuário, a exclusão de dados pessoais não é realizada de forma efetiva nos bancos de dados. A visualização dos dados pessoais da conta excluída é bloqueada para outros usuários, porém parte destes dados continua armazenada nos bancos de dados da empresa. Segundo o Instagram (2015, p. 1), apesar da conta do usuário ser excluída “[...] dados podem persistir e aparecer dentro do serviço”, permitindo que possam existir ocorrências de atividades do subgrupo Insegurança.

Apesar do termo de uso delimitar quais são as atividades permitidas aos usuários na rede social, há opacidade dos procedimentos sobre a arbitragem de supostas violações (como a modificação e a exclusão arbitrária de conteúdos gerados por seus usuários), diretamente ligado a questões inerentes aos subgrupos Insegurança, Exclusão e Vigilância.

É possível realizar a coleta de dados através da API, permitindo que possam existir ocorrências de ações de coleta automatizada, por agentes externos ao sítio, sem o consentimento prévio do usuário (pois são permissivos novos acordos com empresas parceiras, ao longo do tempo), podendo desencadear atividades vinculadas ao subgrupo Quebra de Sigilo.

Não é transparente ao usuário se a rede social compartilha metadados dos conteúdos multimídia de usuários com empresas parceiras. Caso estes metadados sejam compartilhados, é possível agregá-los com dados pessoais, garantindo a estas empresas parceiras informações

adicionais, como: a localização geoespacial e temporal do conteúdo, atividade que é parte do subgrupo Agregação.

Twitter

No termo de uso da rede social Twitter, dados pessoais como o nome, o nome de usuário, a foto do perfil e a localização são, por padrão, parte integrante de um catálogo de dados públicos. O serviço não possui um local apropriado para que usuários observem quais, como, onde e por quem estes conjuntos de dados são coletados e com quais outras fontes de dados são agregados, portanto parte integrante de possíveis ocorrências de atividades dos subgrupos Agregação e Apropriação.

O usuário não tem conhecimento pleno sobre quais são as empresas parceiras que acessam suas informações, sendo possível vincular este tipo de atividade ao subgrupo Aumento do Acesso.

Não é possível delimitar de forma transparente quais informações são geradas por empresas parceiras a partir de dados de usuários ou a forma que manipulam e processam estes dados pessoais com outras fontes de dados, o que pode acarretar atividades ligadas aos subgrupos Uso Secundário e Agregação.

As configurações do Twitter estão ajustadas, por padrão, em um modelo que todo o conteúdo publicado por seus usuários torna-se público a qualquer interessado, sem a necessidade de identificação para o acesso e coleta dos dados, sendo possível a realização de atividades de terceiros que prejudiquem a privacidade através da opacidade da divulgação de informações, que são (aparentemente) íntimas, mas que podem ser expostas ou até retransmitidas de forma incompleta. Estas atividades estão vinculadas aos subgrupos Divulgação, Exposição e Uso Secundário.

5.2. Resultados da aplicação da Taxonomia da Privacidade

O Gráfico I apresenta a síntese da quantidade de potenciais atividades prejudiciais que foram vinculadas a trechos nos termos de uso, agrupados em cada rede social. A sua estrutura está dividida em três colunas, cada uma delas representando a quantidade de subgrupos identificados para a rede social. Foi considerado que, caso o subgrupo tenha sido vinculado a um trecho ao menos uma vez, é somado o valor 1, caso contrário, 0 – não acumulativo por reincidência.

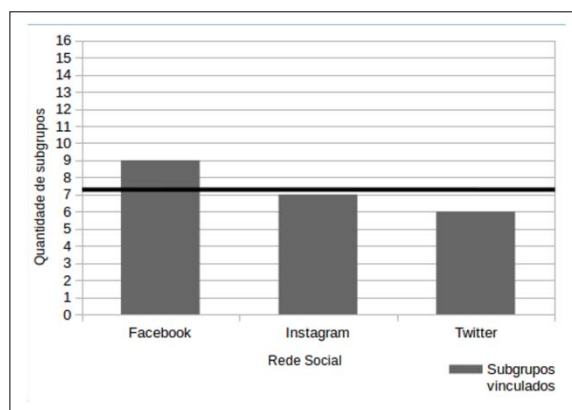


Gráfico I. Quantidade de subgrupos vinculados a trechos de termos de uso, agrupados por rede social

A Taxonomia da Privacidade possui um total de 16 subgrupos, sendo que as redes sociais (colunas) apresentaram totais de vínculos entre 9 e 6, com uma média aproximada de 7,34 (linha horizontal, em evidência) vinculações com subgrupos por rede social.

Os termos de uso apresentaram ao menos uma incidência nos subgrupos Agregação, Uso Secundário, Aumento do Acesso, Vigilância, Insegurança, Exclusão, Quebra de Sigilo, Apropriação, Identificação, Divulgação e Exposição, totalizando 22 (vinte e duas) vinculações com subgrupos, quando somado as três colunas.

O Quadro II sistematiza subgrupos por faixas de incidência, agrupados a partir da quantidade de redes sociais que apresentaram, em seus termos de uso, ao menos um trecho vinculado ao subgrupo.

O quadro está dividido em três colunas: a primeira coluna representa o nome do subgrupo, seguido coluna com a quantidade de redes sociais com termos de uso vinculados com o subgrupo – variando de 0 (quando o subgrupo não fora vinculado a nenhum trecho em nenhum termo de uso) até 3 (quando todos os termos de uso apresentaram, ao menos uma vez, trechos vinculados ao subgrupo).

A terceira coluna, denominada Faixa, estabelece uma divisão por faixas de ocorrências de vinculações destes subgrupos aos termos de uso, onde é delimitado que: a Faixa I concentra os subgrupos com mais incidências; a Faixa II concentra os subgrupos com incidência intermediária; a Faixa III concentra os subgrupos com baixa incidência, e; a Faixa IV concentra os subgrupos com nenhuma incidência para a amostra.

<i>Subgrupo</i>	<i>Quantidade de Redes Sociais com vínculo</i>	<i>Faixa</i>
Agregação	3	Faixa I
Uso Secundário	3	
Aumento do Acesso	3	
Vigilância	2	Faixa II
Insegurança	2	
Exclusão	2	
Quebra de Sigilo	2	
Apropriação	2	Faixa III
Identificação	1	
Divulgação	1	
Exposição	1	Faixa IV
Interrogatório	0	
Chantagem	0	
Distorção	0	
Intromissão	0	
Interferência Decisional	0	
Total	22	-

Quadro II. *Faixas de subgrupos, agrupados a partir da quantidade de redes sociais que apresentaram trechos vinculados.*

O Quadro III (Anexo 2) apresenta a distribuição dos subgrupos de atividades potenciais prejudiciais à privacidade, divididos pelos grupos propostos na Taxonomia da Privacidade, porém com os subgrupos agrupados por faixas de ocorrências em termos de uso das redes sociais. As linhas representam os grupos da Taxonomia da Privacidade e as colunas as faixas de ocorrências do Quadro II (terceira coluna).

A partir do Quadro III, é possível estabelecer que, nos termos de uso das redes sociais, são: **pontos de maior incidência**, elementos que sustentem a possibilidade de atividades prejudiciais à privacidade dos grupos Processamento de Informação e Disseminação de Informação, principalmente sobre questões ligadas aos subgrupos Agregação, Uso Secundário e Aumento do Acesso; **pontos de média incidência**, elementos que sustentem a possibilidade de atividades prejudiciais à privacidade de todos os grupos (Coleta de Informação, Processamento de Informação, Disseminação de Informação e Invasão), principalmente sobre questões ligadas aos subgrupos Vigilância, Exclusão, Insegurança, Quebra de Sigilo e Apropriação, e; **pontos de baixa incidência**, elementos que sustentem a possibilidade de atividades prejudiciais à privacidade dos grupos Processamento de Informação e Disseminação de Informação, principalmente sobre questões ligadas aos subgrupos Identificação, Divulgação e Exposição.

Os subgrupos Interrogatório (do grupo Coleta de Informação); Chantagem e Distorção (do grupo Disseminação da Informação); Intromissão e Interferência Decisional (do grupo Invasão), compõem os subgrupos **sem incidência** e, portanto, não foram vinculados a nenhum termo de uso.

6. Considerações Finais

A média aproximada de 7 subgrupos identificados em termos de uso (Gráfico 1), de um total de 16 subgrupos, abre espaço para reflexão sobre a necessidade de um maior aprofundamento nestes termos de uso de serviços privados de redes sociais, principalmente em estudos – guiados por estes eixos temáticos de atividades – para auxiliar a explicitação de dados antes ocultos, como quais são as atividades mais recorrentes ou passíveis de realização, e; quais possíveis lacunas nos termos de uso destas redes, que podem garantir a legalidade da realização de potenciais atividades prejudiciais à privacidade de usuários.

Concluiu-se que a aplicação de uma taxonomia apropriada pode auxiliar no estudo de termos de uso, possibilitando a explicitação de atividades previstas nestes termos, o que permite inclusive, propostas de futuras aplicações desta metodologia em outros contextos.

A aplicação da Taxonomia da Privacidade também permitiu a reorganização destes subgrupos vinculados a trechos dos termos de uso, a partir de uma classificação por faixas de ocorrências (Quadro II) – onde esta classificação apresenta as possíveis atividades mais recorrentes nos termos de uso (Faixa I) até possíveis atividades que não foram verificadas (Faixa IV). Estas faixas podem auxiliar, por exemplo, na elaboração de estratégias de atualização dos termos de uso destes serviços, através da apresentação de focos de atividades prejudiciais mais aderentes às redes sociais.

Como trabalhos futuros, destacam-se as possibilidades de aplicação deste estudo utilizando termos de uso de outras redes sociais; em outros contextos, como *blogs*, mecanismos de busca, entre outros – e a possibilidade de aplicação destes resultados na definição de estratégias de acompanhamento de atualização destes termos de uso.

Notas

- (1) Tradução da língua inglesa do termo *Online Social Network*.
- (2) Segundo WORLDOMETERS (2015), em 2011 a população mundial superou o número de 7 bi-

lhões, sendo este o valor total adotado neste trabalho.

- (3) Facebook é marca registrada de Facebook Inc.
- (4) A marca Instagram é de propriedade privada de Facebook Inc.
- (5) A marca Twitter é de propriedade privada de Twitter Inc.
- (6) Disponíveis em 20-03-2015.
- (7) As nomenclaturas dos grupos e subgrupos foram traduzidas da língua inglesa para a língua portuguesa pelos autores.
- (8) Quando disponível.
- (9) Tradução da palavra em língua inglesa *decay*.

Referencias

- Adamic, L. A.; Adar, E. (2003). Friends and neighbors on the Web. *Social Networks*, 25(3), 211–230. [http://doi.org/10.1016/s0378-8733\(03\)00009-1](http://doi.org/10.1016/s0378-8733(03)00009-1).
- BBC. (2014, Dezembro 2014). *Instagram now bigger than Twitter*. Recuperado 10-01-2015, de <http://www.bbc.co.uk/newsbeat/article/30410973/instagram-now-bigger-than-twitter>
- Castells, M. (2002). O poder da identidade. São Paulo: Paz e terra.
- Castells, M. (2003). A Sociedade em rede. São Paulo: Paz e Terra.
- CERN. (2015). *The birth of the web*. Recuperado 12-02-2015, de <http://home.web.cern.ch/topics/birth-web>
- Chen, D.; Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference On Computer Science and Electronics Engineering*. <http://doi.org/10.1109/iccsee.2012.193>
- Facebook. (2015a). *Statistics*. Recuperado 10-02-2015, de <http://newsroom.fb.com/company-info/>
- Facebook. (2015b). *Terms of Service*. Recuperado 10-02-2015, de <https://www.facebook.com/legal/terms>
- Facebook. (2015c). *Data Policy*. Recuperado 10-02-2015, de <https://www.facebook.com/about/privacy/>
- Fogel, J.; Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers In Human Behavior*, 25(1), 153–160. <http://doi.org/10.1016/j.chb.2008.08.006>
- Instagram. (2015a). *Terms of Use*. Recuperado 10-02-2015, de <https://help.instagram.com/478745558852511>
- Instagram. (2015b). *API Terms of Use*. Recuperado 10-02-2015, de <https://instagram.com/about/legal/terms/api/>
- Instagram. (2015c). *Privacy Policy*. Recuperado 10-02-2015, de <https://help.instagram.com/155833707900388>
- Krasnova, H.; Günther, O.; Spiekermann, S.; Koroleva, K. (2009). Privacy concerns and identity in online social networks. *IDIS Identity In the Information Society*, 2(1), 39–63. <http://doi.org/10.1007/s12394-009-0019-1>
- Mislove, A.; Marcon, M.; Gummadi, K. P.; Druschel, P.; Bhattacharjee, B. (2007). Measurement and analysis of online social networks. *Proceedings Of the 7th ACM SIGCOMM Conference on Internet Measurement - IMC '07*. <http://doi.org/10.1145/1298306.1298311>
- Santana, R. C. G. (2013). Ciclo de Vida dos Dados e o papel da Ciência da Informação. *XIV Encontro Nacional de Pesquisa em Ciência da Informação '13*. ISBN: 978-85-65044-06-6
- Solove, D. J. (2006). A Taxonomy of Privacy. *University Of Pennsylvania Law Review*, 154(3), 477. <http://doi.org/10.2307/40041279>
- Twitter. (2015a). *Twitter Terms of Service*. Recuperado 10-02-2015, de https://twitter.com/tos/previous/version_8?lang=en
- Twitter. (2015b). *Twitter Privacy Policy*. Recuperado 10-02-2015, de https://twitter.com/privacy/previous/version_9?lang=en
- WORLDMETERS. (2015). *Real Time Statistics*. Recuperado 10-01-2015, de <http://www.worldometers.info/>
- Young, A. L.; Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites. *Proceedings Of the Fourth International Conference on Communities and Technologies – C&T '09*. <http://doi.org/10.1145/1556460.1556499>

Anexo 1

<i>Grupo</i>	<i>Subgrupo</i>	<i>Conceitos de Atividades</i>
Coleta de Informação (Grupo I)	Vigilância	Atividades encadeadas com o propósito de vigiar um indivíduo no seu espaço privado ou em espaço público.
	Interrogatório	Atividades de processos de coleta de dados, baseados em interrogatórios e entrevistas.
Processamento de Informação (Grupo II)	Agregação	Atividades vinculadas ao processo de combinação de dados de múltiplas fontes sobre indivíduos, com o propósito de revelar fatos ocultos, quando eram analisados de forma separada.
	Identificação	Atividades a partir do processo de vinculação de dados que permitam a (re)identificação de usuário (e de seus dados pessoais) com suas respectivas pessoas.
	Insegurança	Atividades que não perpassam segurança sobre questões de acesso a dados pessoais aos envolvidos.
	Uso Secundário	Atividades que envolvem o uso de dados coletados para um determinado propósito e utilizados <i>a posteriori</i> para outras finalidades.
	Exclusão	Atividades que apresentam opacidade ao indivíduo no processo de armazenamento de dados pessoais, no compartilhamento destes dados a terceiros e na ausência ou na inabilidade de participação nas decisões sobre questões envolvendo a coleta, o armazenamento, o uso e o compartilhamento destes dados.
Disseminação de Informação (Grupo III)	Quebra de Sigilo	Atividades em que ocorrem a quebra de confiança entre as partes em manter a confidencialidade das informações sobre indivíduos.
	Divulgação	Atividades de divulgação e de disseminação de informações sobre um indivíduo, que acarretam mudanças na maneira que outros indivíduos julgam seu caráter.
	Exposição	Atividades vinculadas a exposição para terceiros de atributos emocionais ou físicos de intimidade do indivíduo, tais como a nudez, funções corporais e informações de cunho privado.
	Aumento do Acesso	Atividades que visam amplificar o acesso à dados pessoais além do previsto ou do combinado entre as partes.
	Chantagem	Atividades de controle, de dominação, de intimidação ou de ameaças a pessoas ou grupos, por terceiros.
	Apropriação	Atividades que utilizam dados pessoais de um determinado sujeito em benefício de um terceiro ou para cancelar um serviço ou um produto, sem o pleno consentimento do sujeito.
	Distorção	Atividades de disseminação de informações falsas ou interpretadas de maneira dúbia sobre um indivíduo.
Invasão (Grupo IV)	Intromissão	Atividades com o propósito de realizar incursões em assuntos ou em informações de caráter privado.
	Interferência Decisional	Atividades de envolvimento do Estado em assuntos de caráter privado, alterando decisões em nome do indivíduo.

Quadro I. Grupos, subgrupos e conceitos de atividades prejudiciais a privacidade, adaptado de Solove (2006)

Anexo 2

<i>Grupo/Faixa</i>	<i>Faixa I</i>	<i>Faixa II</i>	<i>Faixa III</i>	<i>Faixa IV</i>
Coleta de Informação (Grupo I)		Vigilância		Interrogatório
Processamento de Informação (Grupo II)	Agregação Uso Secundário	Exclusão Insegurança	Identificação	
Disseminação de Informação (Grupo III)	Aumento do Acesso	Quebra de Sigilo	Divulgação Exposição	Chantagem Distorção
Invasão (Grupo IV)		Apropriação		Intromissão Interferência Decisional

Quadro III. *Subgrupos de atividades prejudiciais a privacidade, divididos pela hierarquia da Taxonomia da Privacidade, agrupados por faixas de ocorrências em termos de uso de redes sociais.*