

Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais

Fabício Silva Assumpção

Doutorando; Universidade Estadual Paulista (UNESP);
assumpcao.f@gmail.com

Ricardo Cesar Gonçalves Santana

Doutor; Universidade Estadual Paulista (UNESP);
ricardosantana@marilia.unesp.br

Plácida Leopoldina V.A. da Costa Santos

Doutora; Universidade Estadual Paulista (UNESP);
placida@marilia.unesp.br

Resumo: Considerando a privacidade dos dados dos usuários nas redes sociais, o papel das imagens nas redes sociais e as imagens como fontes de dados, objetiva-se identificar como a coleta de dados a partir de imagens é tratada no Facebook e no Instagram. Para isso, são identificados os principais métodos utilizados para a coleta de dados a partir de imagens no Facebook e no Instagram, as menções à coleta de dados a partir das imagens nas políticas dessas redes sociais, e as opções dos usuários para a configuração desta coleta. Conclui-se que as políticas dessas redes sociais se mostram vagas em diversos momentos no que diz respeito à coleta de dados a partir de imagens, sem especificar quais dados são coletados e listando itens apenas com caráter exemplificativo. Essas conclusões ressaltam a necessidade de conscientização dos usuários de redes sociais acerca de sua privacidade durante a coleta de dados.

Palavras-chave: Privacidade. Coleta de dados. Imagem. Facebook. Instagram.

1 Introdução

O acesso ubíquo à Web, potencializado pelos dispositivos móveis, como os telefones celulares, contribui para uma presença massiva de usuários nas redes sociais. Nessas redes, os usuários criam e consomem conteúdo a todo *instante*, desde o simples clicar ou “curtir” em um *post* ou *link* até o *upload* de uma imagem ou vídeo. No que diz respeito ao uso de imagens em redes sociais – foco deste estudo, no contexto de investigação sobre informação e tecnologia – considera-se que o

crescente uso de telefones celulares do tipo “*smartphone*”, com câmeras cada vez melhores e mais acessíveis, tem sido um dos responsáveis pelo significativo papel que as imagens desempenham nas redes sociais.

Desde os tempos mais remotos, a imagem desempenha um importante papel na sociedade, independentemente das tecnologias utilizadas para sua criação, transmissão e acesso. Potencializada pelas tecnologias de informação e comunicação atuais, a imagem – principalmente a imagem digital – faz cada vez mais parte da vida do ser humano.

Considerando a presença das redes sociais na Web, o papel das imagens digitais nas redes sociais e as próprias imagens como fontes de dados, são levantadas as seguintes questões: “O que acontece com as imagens submetidas pelos usuários nas redes sociais?”, “São coletados dados dessas imagens? Quais dados?”, “Como as redes sociais lidam com as imagens em seus termos de privacidade?”. Essas questões conduzem ao objetivo deste trabalho: identificar como a coleta de dados a partir de imagens é tratada nas redes sociais Facebook¹ e Instagram².

Para alcançar esse objetivo, busca-se, mais especificamente, (1) identificar os principais métodos que são utilizados nas redes sociais para a coleta de dados a partir de imagens, (2) identificar se há menção à coleta de dados a partir das imagens nas políticas das redes sociais Facebook e Instagram, e (3) identificar se nessas redes sociais são apresentadas aos usuários opções para a configuração da coleta de dados a partir das imagens.

O estudo é apresentado em três etapas: (1) uma revisão de literatura em que são abordados brevemente os tópicos que permeiam a questão das imagens em redes sociais e a coleta de dados, (2) uma análise da Política de dados da rede social Facebook (FACEBOOK, 2015) e da Política de privacidade da rede Instagram (INSTAGRAM, 2013), com ênfase na coleta de dados a partir de imagens, e (3) as considerações finais a partir da análise da política de dados e de privacidade.

2 A imagem nas redes sociais: aspectos gerais e coleta de dados

As redes sociais, cada vez mais integradas com outros ambientes digitais e repletas

de recursos, se configuram como espaços com múltiplas funcionalidades. Para Külcü e Henkoglu (2014, p. 761, tradução nossa), as “[...] redes sociais têm um espaço importante entre as ferramentas utilizadas como infraestruturas digitais de informação nas quais ideias, mensagens e notícias pessoais ou institucionais são produzidas, compartilhadas e consumidas, e como uma interface para acessar novas informações.”.

Essas redes podem ser encaradas como espaços muitas vezes públicos para a troca de informações e são cada vez mais presentes na Web. Segundo Liu et al. (2011, p. 61), quase metade dos usuários que têm acesso à Internet são membros de alguma rede social on-line, o que causa uma mudança fundamental nos padrões de troca na Web. “O resultado dessa mudança é que, ao invés de serem apenas consumidores, os indivíduos agora são obrigados a serem criadores e gerenciadores de conteúdo.” (LIU et al., 2011, p. 61, tradução nossa).

O desenvolvimento das tecnologias de informação e de comunicação que trouxe, entre outros, o barateamento do espaço para o armazenamento digital, da conexão com a Internet e dos dispositivos para o acesso e a criação de conteúdo, impulsiona o desenvolvimento dos recursos nas redes sociais. Antes com predominância de conteúdo textual, hoje as redes sociais oferecem recursos para o compartilhamento também de imagens e de vídeos de forma praticamente ilimitada aos seus usuários. Com isso, as redes sociais, como o Facebook, estão cada vez mais permeadas por imagens, facilmente capturadas por dispositivos de baixo custo.

O estudo realizado por Zhao, Grasmuck e Martin (2008³ apud LANG; BARTON, 2015, p. 148) revela que os usuários do Facebook mostram suas identidades através do uso de fotografias ao invés de dizê-las. Lang e Barton (2015) entendem que o álbum fotográfico, tradicionalmente algo particular, tem se tornado algo cada vez mais público. Para as autoras,

O tradicional álbum de fotos, normalmente curado por um membro da família ou amigo e armazenado na privacidade de um lar, está limitado ao alcance das fotos arquivadas dentro de uma localização física. Enquanto as fotografias continuam sendo coletadas em seus álbuns físicos, a Internet mudou o modo com que usamos e compartilhamos imagens. Dois fatores influenciaram a evolução da fotografia de um artefato privado para uma ferramenta de identidade pública: a transição das câmeras analógicas para as digitais e o surgimento da Internet.

(LANG; BARTON, 2015, p. 148, tradução nossa).

Ao interagirem com o ambiente e com outros indivíduos, os usuários das redes sociais geram dados: o conteúdo de suas interações (imagens, textos, vídeos, etc.), os dados sobre esse conteúdo (data, local, etc.) e os dados sobre os usuários relacionados ao conteúdo (endereço de IP, dispositivo, etc.). Assim, uma vez que as redes sociais adquirem aspectos de espaços públicos, surgem questões relacionadas à privacidade dos dados criados pelos ou sobre os usuários das redes sociais.

Hoje, para cada porção individual de conteúdo compartilhado em sites como o Facebook – cada *post*, foto, atualização de status e vídeo do mural – o *uploader* deve decidir quais de seus amigos, membros de grupos ou demais usuários do Facebook poderão acessar o conteúdo. (LIU et al., 2011, p. 61, tradução nossa).

Enquanto a facilidade tecnológica, de um lado, impulsiona o uso de imagens em redes sociais, do outro, as empresas gestoras das redes sociais parecem incentivar e, porque não, direcionar os usuários para uma publicidade cada vez maior de seus dados. Para ilustrar essa observação, cabe mencionar a alteração realizada no Facebook em dezembro de 2009 (BANKSTON, 2009; FACEBOOK..., 2009).

[...] As novas mudanças do Facebook são obviamente planejadas para fazer com que as pessoas abram ainda mais seus dados do Facebook para o público. A “ferramenta de transição” da privacidade, que guia o usuário através das configurações, “recomendará” – pré-selecionará por padrão – a configuração de compartilhar o conteúdo postado pelo usuário, como as mensagens de status e os *posts*, com qualquer usuário da Internet, mesmo quando o nível padrão de privacidade anteriormente configurado pelo usuário estava limitado à “Sua rede e amigos” [...] (BANKSTON, 2009, tradução nossa).

Essa alteração foi aplicada para cerca 350 milhões de usuários que, na época, mantinham perfis na rede social (FACEBOOK..., 2009). Embora o Facebook tenha notificado os usuários sobre a alteração por meio de um *pop-up* e pedido que eles atualizassem suas configurações de privacidade, entende-se que muitos não o fizeram, mantendo, assim, as opções padrão para o compartilhamento com “todos”. Além disso, os usuários que criaram perfis após 2009, já ingressaram na rede social compartilhando, por padrão, seus posts, imagens e vídeos com todos.

As opções de configuração de privacidade em redes sociais, como o Facebook, transmitem ao usuário a sensação de controle sobre seus dados pessoais.

No entanto, cabe destacar que tais configurações, em sua maioria, cobrem apenas os aspectos relacionados ao acesso aos dados – quais dados podem ser acessados e por quem –, abrangendo, assim, apenas uma das fases do ciclo de vida dos dados: a recuperação.

Para os propósitos desse estudo, entende-se que o ciclo de vida dos dados compreende quatro fases: coleta, armazenamento, recuperação e descarte, fases estas que se relacionam à privacidade, à qualidade, aos direitos autorais, à integração, à disseminação e à preservação dos dados (SANTANA, 2013, p. 15).

Explicando o ciclo de vida dos dados, Santana (2013, p. 17) aponta que “[...] a fase de coleta permite que seja iniciada a fase de armazenamento que por sua vez propicia a execução da fase de recuperação e ainda pode gerar novos dados retomando ações da fase de coleta.”.

Na fase de coleta têm-se as atividades vinculadas à definição inicial dos dados a serem utilizados, seja na elaboração do planejamento de como serão obtidos, filtrados e organizados, identificando-se a estrutura, formato e meios de descrição que será utilizado. Nesta fase o dado deve ainda ser devidamente descrito em metadados, avaliados e selecionados. (SANTANA, 2013, p. 18).

Partindo da preocupação com a privacidade dos dados dos usuários em redes sociais, a literatura apresenta uma variedade de estudos. Embora cada estudo tenha seu diferencial em relação aos demais, seja pelas variáveis ou pelos contextos analisados, é possível observar a predominância dos estudos sobre a privacidade no acesso aos dados dos usuários. Esses estudos, entre eles Liu et al. (2011), Kisekka, Bagchi-Sen e Rao (2013), Young e Quan-Haase (2013), Cermak, Smutny e Janoscik (2014), Külçü e Henkoglu (2014), Wolf, Willaert e Pierson (2014) e Lang e Barton (2015), tratam, principalmente, de questões como “quem está acessando os dados dos usuários?”, “quais dados dos usuários são disponibilizados abertamente?”, “o que é feito com esses dados?”, “os usuários definem quem terá acesso aos seus dados?” e “quais estratégias são utilizadas pelos usuários para assegurar a privacidade de seus dados?”. Esses estudos podem ser considerados, sob a perspectiva do ciclo de vida dos dados destacado por Santana (2013), estudos voltados à fase da recuperação dos dados.

Entende-se, no entanto, que a preocupação com a privacidade dos dados dos

usuários de redes sociais deve acentuar-se também na fase da coleta e não somente na recuperação ou no acesso a esses dados, principalmente considerando que a fase da coleta permite que as demais fases ocorram e que, a partir do momento em que os dados foram coletados, o usuário não dispõe de meios que o assegurem que seus dados não serão utilizados para propósitos além daqueles consentidos ou conhecidos por ele. Ou seja, a partir do momento em que seus dados são coletados, o usuário pode perder o controle sobre eles.

Para exemplificar a necessidade de considerar a privacidade durante a coleta dos dados, Johnston e Wilson (2012) descrevem a funcionalidade “Encontrar amigos” do Facebook. Com essa funcionalidade, um usuário da rede social pode informar o endereço de e-mail e senha utilizados por ele em um provedor de e-mail e, partir desses dados, o Facebook armazena a lista de contatos do usuário, contatos esses que, segundo o próprio Facebook (COMO..., 2015), “[...] podem ser usados para ajudar outras pessoas a localizar amigos ou para gerar sugestões de amizade para você e para outros usuários.”. Sobre essa funcionalidade, o Facebook informa ao usuário que sua senha não será armazenada, apenas utilizada para a importação dos dados.

Embora seja importante que o Facebook prometa que não reterá uma cópia da senha do e-mail do usuário, este pode ser o menor dos problemas de privacidade. O que nos preocupa mais é que a importação da lista de contatos representa uma coleta indireta de informações pessoais pelo Facebook sem a autorização (ou mesmo conhecimento) dos indivíduos envolvidos. (JOHNSTON; WILSON, 2012, p. 61, tradução nossa).

Para os autores, além de prover ao Facebook acesso à lista de contatos, que pode vir a ser utilizada para outros propósitos além daquele de facilitar o relacionamento na rede social, a própria funcionalidade “Encontrar amigos”, dentro de seu propósito, pode violar a privacidade dos indivíduos que fazem parte da lista de contatos, expondo-os e sugerindo os relacionamentos entre eles na rede social (JOHNSTON; WILSON, 2012).

Johnston e Wilson (2012) destacam também que “Encontrar amigos” é uma das primeiras coisas às quais o usuário é apresentado após realizar o cadastro na rede social, o que o induz ainda mais ao uso dessa funcionalidade.

Partindo do exemplo da funcionalidade “Encontrar amigos”, considera-se que o entendimento acerca da coleta, incluindo os métodos utilizados para tanto e das possibilidades de controle sobre a coleta, faz-se essencial para a discussão das questões relacionadas à privacidade dos dados dos usuários em redes sociais, inclusive, das imagens criadas e/ou compartilhadas por esses usuários.

No âmbito das imagens digitais, entende-se que a coleta de dados sobre as imagens pode ocorrer por distintos meios. Na literatura, na Política de dados do Facebook (FACEBOOK, 2015) e na Política de privacidade do Instagram (INSTAGRAM, 2013) é possível identificar alguns desses meios, tais como:

- a) reconhecimento facial: identificação das faces presentes em uma imagem e/ou identificação dos indivíduos aos quais as faces pertencem;
- b) metadados incorporados ao arquivo: metadados no padrão *Exchangeable Image File Format* (EXIF) podem ser incorporados aos arquivos das imagens digitais pelos dispositivos de captura ou por software de edição de imagens; o padrão EXIF apresenta metadados para indicar, por exemplo, fabricante e modelo do dispositivo, data, hora e local de captura da imagem (SOCIAL..., 2013);
- c) identificação do dispositivo de origem através do padrão de ruído do sensor: o *Sensor Pattern Noise* (SPN) (padrão de ruído do sensor) é considerado a “impressão digital” dos dispositivos de captura e, através dele, é possível associar as imagens aos dispositivos a partir dos quais foram capturadas (LUKAS; FRIDRICH; GOLJAN, 2006); Satta e Stirparo (2014) descrevem o uso do SPN para a vinculação de imagens digitais a perfis de redes sociais;
- d) dados da conexão e do dispositivo: dados como o endereço de IP e o endereço MAC, a data e o horário da conexão, a marca, o modelo e as configurações do dispositivo podem ser coletados e associados às imagens digitais;
- e) vinculação com dados anteriormente coletados: a partir da vinculação de dados previamente coletados, é possível coletar dados sobre as imagens; por exemplo: o usuário “U” foi identificado em uma imagem “I”, a imagem “I” foi capturada na data “D”, na data “D” o usuário “U” estava no local “L”,

portanto, a imagem “I” foi capturada no local “L”.

Nas seções seguintes, são apresentadas as duas redes sociais, Facebook e Instagram, e os fragmentos de suas políticas de dados e de privacidade que, implícita ou explicitamente, tratam da coleta de dados a partir de imagens digitais. Nesses fragmentos, buscou-se identificar os métodos utilizados para a coleta dos dados, tanto aqueles mencionados acima quanto outros métodos que pudessem ser empregados nessas redes sociais.

3 Política de dados do Facebook

O Facebook foi criado em 2004 por Mark Zuckerberg como uma rede social, inicialmente, limitada aos alunos da Universidade de Harvard. Desde então, o Facebook tem crescido em quantidade de usuários e se destacado como a maior rede social online já existente. Em dezembro de 2014, o Facebook contou com a média diária de 890 milhões de usuários ativos, distribuídos ao redor do planeta, dos quais 745 milhões acessaram a rede social através de disponíveis móveis (FACEBOOK, 2014). Com isso, o Facebook está listado como o segundo site mais acessado da Web em todo o mundo e o segundo site mais acessado no Brasil (ALEXA, 2015).

A partir de 30 de janeiro de 2015, passou a vigorar no Facebook uma nova versão de sua Política de dados (FACEBOOK, 2015). A seguir, são destacados os pontos dessa nova versão identificados como relacionados à coleta de dados a partir de imagens na rede social.

A Política de dados do Facebook é apresentada em oito seções, identificadas por questões: “Quais tipos de informações coletamos?”, “Como usamos essas informações?”, “Como estas informações são compartilhadas?”, “Como faço para gerenciar ou excluir informações sobre mim?”, “Como respondemos a solicitações judiciais ou evitamos danos?”, “Como os nossos serviços globais operam”, “Como lhe notificaremos sobre mudanças nesta política?” e “Como entrar em contato com o Facebook em caso de dúvidas” (FACEBOOK, 2015). Cada seção possui uma quantidade variada de subseções.

Na seção “Quais tipos de informações coletamos?”, a subseção “O que você

faz e as informações que fornece” da política menciona diretamente a coleta de dados:

Coletamos o conteúdo e outras informações transmitidas por você quando usa nossos Serviços, incluindo quando se cadastra em uma conta, cria ou compartilha conteúdos, envia mensagens ou se comunica com os outros. Isso pode incluir informações presentes no conteúdo ou a respeito dele, como a **localização de uma foto** ou a **data que um arquivo foi criado**. Também coletamos informações sobre como você usa nossos Serviços, por exemplo, os tipos de conteúdo que você vê ou com que se envolve e a frequência ou duração de suas atividades. (FACEBOOK, 2015, grifo nosso).

Entende-se que este trecho da política, assim como os demais apresentados a seguir, aborda a questão da coleta de dados de forma vaga, sem especificar exatamente quais são os dados coletados. Os itens listados são sempre de carácter exemplificativo. O exemplo da coleta da “localização de uma foto” não evidencia como tal dado é obtido pelo Facebook: se é através da marcação realizada pelo usuário, pelos dados EXIF de localização incorporados à imagem, pelos dados de localização da rede do dispositivo, ou a partir de qualquer outro método.

Na seção “O que os outros fazem e as informações que fornecem”, a política declara que:

Também **coletamos conteúdos e informações transmitidas por outras pessoas** durante o uso dos nossos Serviços, incluindo informações sobre você, por exemplo, **quando elas compartilham fotos suas**, enviam mensagens a você, ou carregam, sincronizam ou importam suas informações de contato. (FACEBOOK, 2015, grifo nosso).

Este trecho da política reforça o entendimento de que a privacidade dos dados de um indivíduo não depende exclusivamente de sua ação na rede social. Um usuário da rede de social, por exemplo, pode optar por manter alguns de seus dados privados, enquanto que esses dados podem ser expostos por algum indivíduo de seu círculo de amigos, como acontece com a funcionalidade “Encontrar amigos”, comentada anteriormente. A declaração presente na seção “Como usamos essas informações?” reforça esse entendimento:

Também usamos as informações que temos para fornecer atalhos e sugestões para você. Por exemplo, podemos sugerir que um amigo marque você em uma foto examinando e comparando fotos do seu amigo com informações que reunimos **a partir das suas fotos** de perfil e de outras fotos em que você tenha sido marcado. (FACEBOOK, 2015, grifo nosso).

Essa declaração é acompanhada de “[...] você poderá controlar se sugerirmos que outro usuário marque você em uma foto, usando as configurações de ‘Linha do Tempo e marcações’” (FACEBOOK, 2015). Num primeiro momento, essa declaração pode conduzir ao entendimento de que o usuário controla a coleta dos dados. O que está sob o controle do usuário, no entanto, é a possibilidade de que outros indivíduos, nesse caso seus amigos, acessem o produto da coleta, que é a própria possibilidade de identificar um indivíduo. Em nenhum momento são apresentadas ao usuário opções como “Não desejo que o Facebook identifique-me nas fotos dos meus amigos” ou “Não desejo que o Facebook analise minhas fotos na tentativa de identificar-me ou de identificar meus amigos”.

A identificação de indivíduos em fotos no Facebook é realizada através de um sistema de reconhecimento facial, que consiste na análise de uma imagem na tentativa de encontrar características que levem à identificação de uma pessoa. Uma vez que o sistema analisa uma imagem na tentativa de extrair dados dela, entende-se aqui que o reconhecimento facial é uma das técnicas para a coleta de dados, mesmo que os dados coletados tenham sido descartados.

Em um recente artigo (TAIGMAN et al., 2014), de autoria de pesquisadores do *Facebook AI Research* e da *Tel Aviv University*, é apresentado o sistema *DeepFace*. Segundo os autores, o reconhecimento facial consiste de quatro estágios: detectar, alinhar, representar e classificar. No sistema *DeepFace*, os autores empregaram modelagem facial em 3D e redes neurais no alinhamento e na representação, respectivamente, o que permitiu a eles alcançar uma precisão de acerto de 97,35% na identificação de quatro milhões de faces que pertenciam a mais de 4 mil identidades (TAIGMAN et al., 2014). Embora o sistema *DeepFace* tenha sido desenvolvido por membros do *Facebook AI Research*, órgão “[...] comprometido com o avanço do campo da inteligência da máquina e com o desenvolvimento de tecnologias que dão às pessoas melhores formas de se comunicar.” (FACEBOOK AI RESEARCH, 2015, tradução nossa), não foi localizada qualquer menção ao seu uso na rede social.

A política de dados do Facebook menciona também a coleta de dados do dispositivo:

Coletamos informações de ou sobre computadores, telefones e outros dispositivos em que você instala ou acessa nossos Serviços, dependendo das **permissões** concedidas. Podemos associar as informações coletadas dos seus diferentes dispositivos, o que nos ajuda a fornecer Serviços consistentes entre dispositivos. Veja alguns exemplos das informações que coletamos sobre os dispositivos:

- [...]
- Localizações do dispositivo, incluindo localizações geográficas específicas, por meio de GPS, Bluetooth ou sinal Wi-Fi.
- [...] (FACEBOOK, 2015, grifo nosso).

A declaração de que o Facebook pode, a partir das permissões concedidas, coletar e associar informações sobre os dispositivos com os quais os usuários acessam a rede social abre uma variedade de possibilidades para que sejam coletados dados sobre as imagens. Em dezembro de 2014, o Facebook contou com a média diária de 745 milhões de usuários acessando a rede social via dispositivos móveis (FACEBOOK, 2014). O aplicativo oficial para o acesso ao Facebook para o sistema operacional Android, sistema instalado em uma quantidade significativa dispositivos, requer, entre suas permissões, o acesso à localização precisa e aproximada (por GPS e com base na rede) e permissão para ler, alterar ou excluir conteúdo armazenado (imagens, mídia, arquivos) e para capturar imagens e vídeos (GOOGLE PLAY, 2015).

4 Política de privacidade do Instagram

O Instagram, diferentemente do Facebook, foi concebido como uma rede social para o compartilhamento de imagens através de dispositivos móveis, tendo entre suas principais características a possibilidade de adicionar filtros de cor, brilho, contraste, saturação etc. às imagens. Criado em outubro 2010, hoje o Instagram conta com cerca de 300 milhões de usuários ativos mensalmente e com mais de 30 bilhões de fotos compartilhadas (INSTAGRAM, 2015). Em abril de 2012, o Instagram foi adquirido pelo Facebook.

A política de privacidade do Instagram (INSTAGRAM, 2013) refere-se às imagens como sendo “*User content*”, ou seja, “o conteúdo do usuário”, que inclui “fotos, comentários e outros materiais”. Essa política inclui as seguintes seções: “Informações que coletamos”, “Como usamos suas informações”,

“Compartilhamento de suas informações”, “Como armazenamos suas informações”, “Suas escolhas sobre suas informações”, “Privacidade de crianças”, “Outros websites e serviços”, “Como nos contatar sobre um usuário falecido”, “Como nos contatar” e “Mudanças em nossa política de privacidade”.

Sobre a coleta de dados a partir do conteúdo do usuário, a política de privacidade do Instagram apresenta apenas o seguinte trecho:

Metadados:

Metadados normalmente são dados técnicos associados ao conteúdo do usuário. Por exemplo, os metadados podem descrever como, quando e por quem uma porção do conteúdo do usuário foi coletada e como esse conteúdo está formatado.

Usuários podem adicionar ou ter metadados adicionados ao seu conteúdo incluindo uma *hashtag* (e.g., para marcar palavras-chave quando você posta uma foto), uma *geotag* (e.g., para marcar sua localização em uma foto), comentários ou outros dados. Isso faz seu conteúdo mais pesquisável por outros usuários e mais interativo. Se você inclui uma *geotag* em sua foto ou uma *tag* usando outras APIs, sua latitude e longitude serão armazenadas com a foto e se tornarão pesquisáveis (e.g., através da localização ou do mapa) se sua foto está pública de acordo com suas configurações de privacidade. (INSTAGRAM, 2013, tradução nossa).

A primeira sentença do fragmento, “Metadados normalmente são dados técnicos que estão associados ao conteúdo do usuário”, conduz ao entendimento de que a política pode estar se referindo aos metadados que acompanham as imagens digitais, tais como os metadados do padrão EXIF. No entanto, o restante do fragmento da política enfatiza os metadados que podem ser adicionados ao conteúdo, por exemplo, as *tags* (ou *hashtags*) e os dados sobre localização. Esses metadados acrescentados ao conteúdo, por persistirem no sistema de modo a possibilitar a recuperação das imagens, obviamente, são coletados. O que a política não deixa claro é o tratamento que os dados técnicos associados às imagens recebem e quais são esses dados.

Sobre a coleta de dados a partir dos metadados presentes em um arquivo de imagem, são destacados aqui os resultados do estudo publicado no *Embedded Metadata Manifesto* (SOCIAL..., 2013). O estudo teve entre seus objetivos verificar se, após o upload, os sistemas dos sites de mídia social mantinham nas imagens ou exibiam os metadados que nelas constavam antes do upload. Os sites analisados foram: 500px (<http://500px.com>), Dropbox (<http://www.dropbox.com>), Facebook,

Flickr (conta gratuita) (<http://www.flickr.com>), Google+ (<https://plu.google.com>), Img.ly (<http://img.ly>), Instagram, Joomeo (<http://www.joomeo.com>), Photobucket (<http://photobucket.com>), Pictify (<http://pictify.com>), Pinterest (<http://br.pinterest.com>), Tumblr (<https://www.tumblr.com>), Twitpic (<http://twitpic.com>), Twitter (<http://twitter.com>), Via.me (<http://www.via.me>) e Yfrog (<http://yfrog.com>). Os resultados para o Facebook e o Instagram mostram que todos os metadados foram removidos das imagens, sem a possibilidade de visualizá-los no site ou no próprio arquivo (após o *download*). Neste estudo, não foram localizadas informações sobre o paradeiro dos metadados removidos dos arquivos, ou seja, não se sabe se são descartados ou armazenados.

5 Gerenciamento da coleta

Após a análise das políticas do Facebook e do Instagram, questionou-se quais opções para o gerenciamento da coleta dos dados a partir das imagens essas redes sociais apresentam aos seus usuários. Em busca de respostas a esse questionamento, foram observadas as opções de configuração de privacidade presentes nas redes sociais estudadas.

No Facebook, não foram identificadas opções para o gerenciamento da coleta por meio do reconhecimento facial. Sobre isso, a única possibilidade do usuário é definir quem receberá sugestões de marcações quando imagens suas forem enviadas à rede social, ou seja, ao usuário é dado o controle somente sobre o acesso, sobre a recuperação de seus dados, e não sobre a coleta deles.

Sobre os dados de localização, no Instagram e no Facebook o usuário pode optar por incluir ou não a localização da imagem. Sobre a coleta de dados a partir dos metadados presentes no arquivo digital, não foi encontrada qualquer opção nas duas redes sociais.

Embora a coleta de dados não seja contemplada de forma clara nas políticas estudadas e não sejam apresentadas aos usuários muitas opções para a configuração dessa coleta, as redes sociais, de modo geral, permitem que os usuários configurem o acesso aos seus dados, por exemplo, quem poderá visualizar os posts, as imagens

ou as informações de contato. Apesar dessa possibilidade, nem sempre os usuários chegam a alterar as configurações, mantendo-as sempre com as opções padrão. Albeshier e Alhussain (2013, p. 8, tradução nossa) destacam três razões pelas quais os usuários não alteram as configurações:

Em geral, há três razões por detrás da relutância em ajustar as configurações de privacidade. A primeira razão é o desconhecimento dos usuários dos potenciais riscos que podem resultar de sua falta de cuidado. [...] A segunda razão é o tempo demandado para a leitura e o entendimento de cada configuração. O Facebook é um website muito grande que precisa de vários tipos de configurações de privacidade para prover uma rede poderosa. A diversidade de configurações de privacidade torna a tarefa de modifica-las muito complicada. Essa complexidade é a terceira razão pela qual as configurações não são alteradas. Assim, as configurações de privacidade não têm significado se elas não são cuidadosamente alteradas pelos usuários.

Com isso, apenas garantir a existência da possibilidade não é suficiente, é necessário torná-la explícita ao usuário e acessível do ponto de vista cognitivo, no sentido de que o usuário compreenderá o que está configurando.

6 Considerações finais

A facilidade com que as imagens são hoje capturadas e compartilhadas em redes sociais como o Facebook e o Instagram contribui para o empoderamento das corporações gestoras dessas redes. Um exemplo desse empoderamento é que, juntos, Facebook e Instagram, podem constituir um dos maiores bancos de dados de imagens do mundo, principalmente por terem dados como “quem”, “quando”, “onde” e “o que” agregados a essas imagens – dados esses coletados por meio de reconhecimento facial, dos metadados, dos dados de localização e das *tags*. Com isso, assegurar que os usuários tenham, ao menos, um mínimo controle sobre a coleta de seus dados pessoais faz-se uma tarefa de considerável importância.

Os estudos relacionados à privacidade dos usuários em redes sociais, em especial no Facebook, focam a privacidade dos dados durante a fase de recuperação, ou seja, as preocupações são, principalmente, quem está acessando ou visualizando os dados dos usuários e quais são esses dados. O que nota-se com isso é a falta de estudos sobre a privacidade durante a coleta dos dados. Neste estudo defende-se que a privacidade deve também ser discutida na coleta, pois o usuário de uma rede

social deve ter a oportunidade de consentir ou não a coleta de alguns de seus dados e não somente ficar limitado às opções de acesso após a coleta.

Na defesa deste entendimento, o estudo realizado permitiu concluir que a política de dados do Facebook (2015) e a política de privacidade do Instagram (2013) mostram-se vagas, em diversos momentos, no que diz respeito à coleta de dados a partir de imagens, sem especificar quais dados são coletados e listando itens apenas com caráter exemplificativo. Observa-se também que, apesar de o Instagram ter como principal objetivo possibilitar o compartilhamento de imagens entre seus usuários, tal rede social tem em sua política de privacidade poucas menções à coleta de dados a partir de imagens, se comparada à política de dados do Facebook.

Por fim, nessas considerações, destaca-se que este é um diagnóstico inicial das redes sociais Facebook e Instagram sobre a coleta de dados a partir de imagens, sendo necessário, para o aprofundamento desse diagnóstico e para a proposição de soluções, analisar outros ambientes e variáveis. Com essa abordagem inicial, espera-se favorecer estudos posteriores, no interior da Ciência da Informação, que envolvam ações para a conscientização dos usuários das redes sociais quanto à privacidade dos seus dados.

Referências

ALBESHER, Abdulmohsen; ALHUSSAIN, Thamer. Privacy and Security Issues in Social Networks: An Evaluation of Facebook. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND DESIGN OF COMMUNICATION, 2013. **Proceedings...** p. 7-10, 2013. Disponível em: <<http://dl.acm.org/citation.cfm?id=2503861>>. Acesso em: 25 jan. 2015.

ALEXA. **Facebook.com**. 2015. Disponível em: <<http://www.alexa.com/siteinfo/facebook.com>>. Acesso em: 2 fev. 2015.

BANKSTON, Kevin. Facebook's New Privacy Changes: The Good, The Bad, and The Ugly. **Electronic Frontier Foundation**, December 9, 2009. Disponível em: <<https://www.eff.org/pt-br/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>>. Acesso em: 25 jan. 2015.

CERMAK, Radim; SMUTNY, Zdenek; JANOSCIK, Vaclav. Analysis of Facebook Privacy Settings of Young People With an Emphasis on Czech Republic and France. In: EUROPEAN CONFERENCE ON SOCIAL MEDIA (ECSM), 2014, Brighton.

Proceedings... 2014. Disponível em:

<http://www.researchgate.net/publication/263619922_Analysis_of_Facebook_privacy_settings_of_young_people_with_an_emphasis_on_Czech_Republic_and_France>. Acesso em: 25 jan. 2015.

COMO funciona. Facebook, 2015. Disponível em:

<<https://www.facebook.com/contact-importer/how-it-works/>>. Acesso em: 02 fev. 2015.

FACEBOOK AI RESEARCH. **About Facebook AI Research**. 2015. Disponível em: <<https://research.facebook.com/ai>>. Acesso em: 2 mar. 2015.

FACEBOOK faces criticism on privacy change. Londres: BBC, 10 December 2009. Disponível em: <<http://news.bbc.co.uk/2/hi/8405334.stm>>. Acesso em: 25 jan. 2015.

FACEBOOK. **Our Mission**. Menlo Park, 2014. Disponível em:

<<http://newsroom.fb.com/company-info/>>. Acesso em: 25 jan. 2015.

FACEBOOK. **Política de Dados**. Menlo Park, 2015. Disponível em:

<<https://www.facebook.com/about/privacy/>>. Acesso em: 5 jan. 2015.

GOOGLE PLAY. **Facebook**. 12 de março de 2015. Disponível em:

<<https://play.google.com/store/apps/details?id=com.facebook.katana>>. Acesso em: 14 mar. 2015.

INSTAGRAM. **Página de imprensa**. 2015. Disponível em:

<<http://instagram.com/press/>>. Acesso em: 1 fev. 2015.

INSTAGRAM. **Privacy Policy**. 2013. Disponível:

<<http://instagram.com/about/legal/privacy/>>. Acesso em: 25 jan. 2015.

JOHNSTON, Anna; WILSON, Stephen. Privacy compliance risks for Facebook.

Technology and Society Magazine, IEEE, v. 31, n. 2, p. 59-64, 2012. Disponível em: <<http://dx.doi.org/10.1109/MTS.2012.2185731>>. Acesso em: 25 jan. 2015.

KISEKKA, Victoria; BAGCHI-SEN, Sharmistha; RAO, H. Raghav. Extent of private information disclosure on online social networks: An exploration of

Facebook mobile phone users. **Computers in Human Behavior**, v. 29, p. 2722-2729, 2013. Disponível em: <<http://dx.doi.org/10.1016/j.chb.2013.07.023>>. Acesso em: 25 jan. 2015.

KÜLCÜ, Özgür; HENKOGLU, Turkey. Privacy in social networks: An analysis of Facebook. **International Journal of Information Management**, v. 34, p. 761-769, 2014. Disponível em: <<http://dx.doi.org/10.1016/j.ijinfomgt.2014.07.006>>. Acesso em: 25 jan. 2015.

LANG, Caroline; BARTON, Hannah. Just untag it: Exploring the management of undesirable Facebook photos. **Computers in Human Behavior**, v. 43, p. 147-155, 2015. Disponível em: <<http://dx.doi.org/10.1016/j.chb.2014.10.051>>. Acesso em: 25 jan. 2015.

LIU, Yabing et al. Analyzing Facebook Privacy Settings: User Expectations Vs. Reality. In: ACM SIGCOMM Conference on Internet Measurement Conference, 2011, New York. **Proceedings...** p. 61-70. Disponível em: <<http://www.mpi-sws.org/~gummadi/papers/imc081s-liu.pdf>>. Acesso em: 25 jan. 2015.

LUKAS, J.; FRIDRICH, J.; GOLJAN, M. Digital camera identification from sensor pattern noise. **IEEE Transactions on Information Forensics and Security**, v. 1, n. 2, p. 205-214, 2006. Disponível em: <<https://harpurpalate.binghamton.edu/ia/publication/FridrichPDF/double.pdf>>. Acesso em: 1 dez. 2014.

SANTANA, Ricardo Cesar Gonçalves. Ciclo de vida dos dados e o papel da Ciência da Informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO (ENANCIB), 14., 2013, Florianópolis. **Anais...** Florianópolis: Universidade Federal de Santa Catarina, 2013. Disponível em: <<http://enancib2013.ufsc.br/index.php/enancib2013/XIVenancib/paper/view/284>>. Acesso em: 1 dez. 2014.

SATTA, Riccardo; STIRPARO, Pasquale. On the usage of Sensor Pattern Noise for Picture-to-Identity linking through social network accounts. In: INTERNATIONAL CONFERENCE ON COMPUTER VISION THEORY AND APPLICATIONS (VISAPP), 9., 2014, Lisboa. **Proceedings...** 2014. Disponível em: <<http://pralab.dice.unica.it/en/node/1005>>. Acesso em: 1 dez. 2014.

SOCIAL Media sites: photo metadata test results. In: EMBEDDED Metadata Manifesto. 2013. Disponível em: <<http://www.embeddedmetadata.org/social-media-test-results.php>>. Acesso em: 25 jan. 2015.

TAIGMAN, Yaniv et al. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In: CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION (CVPR), 2014, Columbus. **Proceedings...** Disponível em: <<https://research.facebook.com/publications/480567225376225/deepface-closing-the-gap-to-human-level-performance-in-face-verification/>>. Acesso em: 25 jan. 2015.

WOLF, Ralf De; WILLAERT, Koen; PIERSON, Jo. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. **Computers in Human Behavior**, v. 35, p. 444-454, 2014. Disponível em: <<http://dx.doi.org/10.1016/j.chb.2014.03.010>>. Acesso em: 25 jan. 2015.

YOUNG, Alyson Leigh; QUAN-HAASE Anabel. Privacy protection strategies on Facebook: The Internet privacy paradox revisited. **Information, Communication**

& Society, v. 16, n. 4, p. 479-500, 2013. Disponível em:

<<http://dx.doi.org/10.1080/1369118X.2013.777757>>. Acesso em: 25 jan. 2015.

Data collection from images: considerations on the users' privacy in social networks

Abstract: Considering the privacy concerns on users' data in social networks, the role of images on social networks and the images as data sources, this paper aims to identify how data collection from images is treated in Facebook and Instagram. For this, we identify the main methods for data collection from images, the mentions to data collection from images in Facebook and Instagram policies, and the options that are presented to users for setting up the data collection from images. We conclude that the policies analyzed are vague in several points regarding to data collection from images: they do not specify which data are collected and just list items with an illustrative purpose. These findings highlight the need for studies and actions to raise awareness of social networks users about their privacy in data collection.

Keywords: Privacy. Data collection. Image. Facebook. Instagram.

Recebido em: 29/03/2015

Aceito em: 23/06/2015



¹ Disponível em: <<https://www.facebook.com>>.

² Disponível em: <<https://instagram.com>>.

³ ZHAO, S.; GRASMUCK, S.; MARTIN, J. Identity construction on Facebook: Digital empowerment in anchored relationships. **Computers in Human Behavior**, v. 24, n. 5, p. 1816–1836, 2008. Disponível em: <<http://dx.doi.org/10.1016/j.chb.2008.02.012>>. Acesso em: 16 jun. 2015.