Privacidade de um Usuário Falecido

Francisco Álisson Véras Damasceno [1], **Paulo Victor Barbosa de Sousa**[2]

[1]Campus Quixadá – Universidade Federal do Ceará (UFC)
Av. José de Freitas Queiroz – 5003 – Quixadá – CE – Brasil

francisco.ally57@gmail.com, paulo.victor@ufc.br

Abstract. *Considering the advancement digital age, personal files and documents are mostly stored in digital accounts. While these accounts ensure data privacy and security for user's lifetime, significant dilemmas arise when someone dies. Issues related to digital heritage, privacy and personality rights emerge as current challenges. In this investigation, we seek to understand why it is still unclear how to handle the data of deceased users, despite attempts to address this issue.*

Resumo. *Com o avanço da era digital, os fichários e documentos dos usuários encontram-se predominantemente armazenados em contas digitais. Embora essas contas garantam a privacidade e a segurança dos dados durante a vida do usuário, surgem dilemas significativos quando ocorre o seu falecimento. Questões relativas ao patrimônio digital, privacidade e direitos de personalidade emergem como desafios prementes. Neste trabalho, procuramos entender por que ainda não está claro como lidar com os dados de usuários falecidos, mesmo com alternativas que tentam resolver essa questão.*

Palavras-chave: Privacidade de dados. Herança digital. Testamento digital.

1. Introdução

Lidar com a privacidade de um usuário falecido suscita discussões de natureza ética e tecnológica sobre a posse, exclusão e proteção de dados. Este trabalho está dividido em duas seções, sendo a primeira sobre o referencial teórico, onde são abordadas subseções que tratam do conceito de dados e privacidade, bem como da relação entre a lei e o contexto *post mortem*. Na conclusão, consolida-se a privacidade, dignidade e personalidade, a segurança dos dados e a questão da herança digital na era digital, além da identificação do motivo pelo qual lidar com os dados desse usuário ainda ser algo à deriva.

2. Referencial Teórico

2.1. Dados e Privacidade

Dados são valores que podem ser utilizados para descrever quantidade, qualidade, fatos, estatísticas, ou seja uma unidade de significado. Tem-se exemplos de dados como: nome, idade, salário, nacionalidade, e-mail, senhas e outros. Além disso, os dados podem ser trabalhados individualmente ou agrupados em estruturas como tabelas para ordenamento que fornecem contextos sobre uma determinada coleção [OECD 2008].

Dentro da informática, os dados podem ser divididos em grupos como: pessoais, sensíveis, genéricos e biométricos. Os dados pessoais servem como identificadores de

uma pessoa, incluindo aqueles citados no parágrafo anterior. Enquanto os dados sensíveis, quando não protegidos adequadamente, podem ter seu uso violado por práticas discriminatórias ou criminosas, visto que são sensíveis à vida de seu usuário, possuindo informações de caráter religioso, filosófico e político [Magrani 2018].

Segundo Luciano Floridi, faz-se necessária a distinção entre o conceito de dados e informações. Dados possuem um conceito amplo e não estruturado, enquanto a informação é um dado tratado, por consolidar um valor social e mercadológico. Por exemplo, um usuário pode acessar um grupo de fotografia em uma determinada rede social, ou seja, um dado. Dessa forma, pode-se inferir a seguinte informação, de que o mesmo apresente interesses em artigos de câmeras, lentes e *flashs* [Magrani 2018].

O direito de reserva a informações pessoais, sensíveis ou biométrica, chama-se de privacidade. Que realiza um papel na construção de cada indivíduo, na qual pode ser definida como sendo, "direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" [Rodotà 2008].

Práticas criminosas ou fraudulentas podem ter sua origem na própria utilização de informações pessoais comprometidas, na qual levanta questões importantes referentes a privacidade da informação. A existência de diversas técnicas de furto de dados, reforça a importância de mantê-los seguros pelo bem de seus usuários. Mesmo que algumas técnicas não tenham surgido com propósitos fraudulentos, sua configuração pode ser usada para propósitos ilegais. Assim sendo, foi sintetizado na Tabela 1, encontrada na próxima página, práticas referentes a privacidade, sua respectiva descrição e qual seu risco ao usuário para melhor compreensão das práticas positivas e negativas.

Outro ponto a se levar em conta é a relação entre a dignidade humana e a privacidade. Nesse contexto, Magrani (2008) comenta que, em respeito ao direito à dignidade humana, é necessário considerar o direito ao reconhecimento, ao respeito e à proteção da existência digna. Essa proteção da dignidade, no campo da informática, dá-se pela segurança e pela tutela dos dados pessoais, assegurando que os dados sensíveis de cada pessoa sejam manuseados com responsabilidade e em conformidade com normas éticas e legais. Nesse sentido, a proteção da privacidade não é apenas uma questão técnica, mas também moral, intrinsecamente ligada ao respeito pela dignidade e pela autonomia de cada ser humano.

Quando se fala sobre informações do usuário, inicialmente nomeados como dados e especialmente sobre os aqueles categorizados como sensíveis, não se deve negligenciar questões de privacidade e segurança. A proteção da dignidade humana em relação aos dados envolve cuidar das informações do usuário, ou seja, sua privacidade, e garantir a segurança contra tentativas de fraude desses dados. Infere-se a importância dessas informações para com a proteção da existência digna daquela pessoa, sendo o próprio usuário a maior autoridade quando relacionado ao que fazer com seus dados. Portanto, a preservação da privacidade se alinha de maneira crucial com a promoção da dignidade humana na era digital.

Table 1. Resumo das práticas e seus riscos para os usuários.

Práticas	Descrição	Risco ao Usuário
Cookies	São porções de informação instaladas no computador de um usuário por um servidor que o usuário visitou.	Facilitadora
Data Mining	Envolve o uso de algoritmos para percorrer grandes bancos de dados e encontrar informações.	Facilitadora
Monitoramento de Funcionários	Pode ser permitido eticamente, para fins de segurança e controle da qualidade.	Risco Necessário
Vigilância Governamental	Envolve um equilíbrio entre a coleta de evidência criminal e a preservação da privacidade.	Risco Necessário
Hackers	São pessoas que invadem sistemas computacionais, baixando scripts e protocolos de ataque.	Ameaça
Vírus	Um programa que se espalha danificando arquivos de dados, e alguns podem destruir arquivos.	Ameaça
Vermes (Worms)	Os vermes podem permitir que indivíduos mal-intencionados consigam acessar um computador remotamente e obter suas informações.	Ameaça

[Barger 2014]

2.2. *Post mortem*

Um sistema que fornece serviços de computação e afins, possivelmente terá um banco de dados para o armazenamento de diversos arquivos pessoais, como sendo as informações dos funcionários da empresa, universidade ou governo. A medida que mais dados são inseridos no sistema, é possível que, ao longo do tempo, o serviço se torne inacessível para alguns usuários. Nesse sentido, surgem-se alguns dilemas, incluindo questões éticas, quando se tenta obter arquivos de um determinado usuário, após o seu falecimento [Barger 2014].

Segundo alguns estudos de caso de Barger (2014), tem-se algumas perguntas que podem ser levantadas para melhor questionamento dessa procedência, tais como:

- Entrega-se as chaves de acesso, e-mail e titularidade para o familiar mais próximo?
- Solicita-se o testamento primeiro?
- Deleta-se os arquivos daquele usuário?

As questões acima, foram levantadas em tributo ao usuário e a relação com seus arquivos, bem como questões sobre a permissão dos dados pela família, validade das contas e documentos digitais, assim como o envolvimento de atividades ilegais. Um exemplo

é se o familiares quiserem os arquivos, poderão mostrar um mandato judicial e caso esses dados não seja importantes, deveria-se apagá-los e fechar a conta do usuário. Essas são algumas procedências de administradores no exército dos Estados Unidos. [Barger 2014]

Através da Lei Geral de Proteção de Dados Pessoais (LGPD) [1], foi instituída a regulamentação das atividades de tratamento de dados pessoais, que estabelece o objetivo de proteger os direitos de liberdade, privacidade e personalidade da pessoa natural. O termo pessoa natural, refere-se a existência de alguém desde o seu nascimento até a sua morte, enquanto o termo *post mortem*, advém do *latim*, e que significa período posterior ou após a morte. Dessa forma, a referida lei ainda não oferece diretrizes definidas para o contexto de tratamento de dados em caráter *post mortem* do usuário, porém pode-se analisar outra norma que consiga alojar o tratamento dessas informações, sendo ela os direitos da personalidade.

O direito de personalidade [2] diz respeito a privacidade, à intimidade, à honra, à imagem e ao nome, cabendo a eles receber um nível de proteção elevado que implica em caracteriza-los como: intransmissíveis, irrenunciáveis, indisponíveis e oponíveis. Tamanha é a sua importância, que mesmo após o falecimento do sujeito de direitos, a tutela jurídica dos direitos de personalidade é mantida. Dessa maneira, surge uma contradição entre esses dois direitos, por exemplo tem-se o direito de personalidade que protege e assegura o nome do indivíduo, enquanto a LGPD, não oferece diretrizes que tratem da informação do falecido usuário, mesmo que entre esses dados, um deles seja o próprio nome.

Mesmo assim ainda há agentes que tentam propor uma outra maneira de lidar com isso, tendo o *Google* essa preocupação como usuário, no caso de falecimento ou inatividade prolongada. O sistema gerenciador de contas inativas[3], adota um planejamento sobre o que acontecerá com os dados quando não puder mais usar a conta *Google*, cabendo ao usuário escolher entre um outro usuário de confiança, que atuaria como um "herdeiro" de seus dados ou a exclusão completa. Isso garante que os usuários da plataforma tenham conhecimento sobre o destino de seus arquivos, contas e senhas [Google Inc. 2023].

De acordo com Santos (2014), a herança digital, é uma coletânea de ativos digitais, como por exemplo: e-mail, fotos, vídeos, contas sociais e outros ficheiros eletrônicos; que são elementos correlacionados a alguém, ou seja, uma vida digital. De acordo com o Código Civil Brasileiro [4], a herança digital é uma parte integrante ao patrimônio de uma pessoa, dessa forma está sujeita às leis de sucessão. Assim, tal herança digital é transmitida aos herdeiros legítimos do falecido. Contudo, a sucessão de bens digitais ainda é discutível no Brasil, devido a ausência de leis específicas para gerir esses bens,

[1] A Lei nº 13.709/18, também conhecida como Lei de Proteção de Dados, foi criada para regular o uso de informações pessoais, inclusive em meios digitais, com o propósito de proteger a liberdade, privacidade e o desenvolvimento pessoal das pessoas.

[2] A Lei nº 10.406, encontra-se disposições relacionadas ao Direito da Personalidade. Esse campo legal garante a proteção de informações, textos, discursos e imagens de indivíduos falecidos ou ausentes, proibindo seu uso não autorizado, a menos que partes legítimas, como cônjuges ou herdeiros, o permitam.

[3] O Gerenciador de contas inativas possibilita que os usuários compartilhem dados de suas contas ou avisem alguém quando suas contas ficarem sem uso por um certo período [Google Inc. 2023].

[4] A Lei nº 10.406/2002. Na sessão de herança, é argumentado que morrendo a pessoa sem testamento, transmite a herança aos herdeiros legítimos; o mesmo ocorrerá quanto aos bens que não forem compreendidos no testamento; e subsiste a sucessão legítima se o testamento caducar, ou for julgado nulo.

incluindo questões em que o falecido destine instruções específicas para a procedência de seus arquivos digitais. [Biguelini 2018]

Por fim, é importante observar que o dilema que surge após a morte de um usuário levanta questões éticas sobre como decidir o destino dos dados do falecido. Além disso, há preocupações relacionadas à legislação que regulamenta o patrimônio digital e sua transmissão aos herdeiros dentro dos parâmetros da lei brasileira. No entanto, as questões relacionadas à privacidade não estão claramente definidas nem protegidas, criando uma lacuna significativa entre o direito à personalidade, que ainda não encontrou seu espaço no ambiente digital, e o controle das informações pessoais, que muitas vezes permanece indefinido, apesar dos esforços das empresas em encontrar soluções digitais para políticas de proteção de dados e privacidade.

3. Conclusões

Os dados são valiosos e podem ser usados para construir informações significativas, mas a privacidade é essencial para garantir que os indivíduos tenham controle sobre suas informações pessoais. Práticas criminosas e fraudulentas estão em ascensão, destacando a importância da segurança dos dados. A proteção da dignidade humana e da privacidade não é apenas uma questão técnica; ela também tem implicações morais, ligadas à dignidade e autonomia de cada ser humano.

Quando se trata de dados *post mortem*, há desafios éticos e legais em relação ao destino dos dados de um usuário após sua morte. A LGPD ainda não fornece orientações claras sobre esse cenário, criando uma lacuna significativa entre o direito à privacidade dos dados e o direito à personalidade, que protege informações como o nome. No entanto, algumas empresas começaram a abordar esse problema, permitindo que os usuários escolham um "herdeiro" para seus dados ou optem pela exclusão completa. A herança digital é reconhecida como parte do patrimônio de uma pessoa, mas as leis de sucessão digital ainda são incipientes no Brasil.

Em suma, fica evidente que a legislação atual não acompanha o ritmo veloz das mudanças digitais, e isso pode resultar em lacunas significativas entre a lei brasileira e os serviços digitais em apenas alguns anos. É crucial abordar essa questão para garantir que os dados de um usuário após sua morte sejam tratados de maneira ética e legal. Contudo, uma solução viável pode ser a implementação de testamentos digitais, permitindo que os usuários expressem seus desejos em relação à posse e proteção de seus dados enquanto ainda estão vivos.

References

Barger, R. N. (2014). *Ética na computação: uma abordagem baseada em casos*. Livros Técnicos e Científicos Editora: LTC.

Biguelini, T. D. (2018). Herança digital: Sucessão do patrimônio cibernético.

Google Inc. (2023). Google. Acessado em 6 de setembro de 2023.

Magrani, E. (2018). *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. Konrad Adenauer Stiftung.

OECD (2008). *OECD Glossary of Statistical Terms*.

Rodotà, S. (2008). *A vida na sociedade de vigilância*. Renovar.