



A ÉTICA E O USO DE DADOS SEM AUTORIZAÇÃO OU CONSENTIMENTO PARA BENEFÍCIO PRÓPRIO

Guilherme Prado ROMA¹
Paula Jurema Piloto LANGHI²

RESUMO: A tecnologia hoje é parte integrante da sociedade e o uso de suas diversas abordagens é essencial ao desenvolvimento humano. A informatização de diversas atividades, transforma a Tecnologia da Informação (TI) em uma área cada vez mais relevante expandindo para diversos setores. A era da informação também trouxe aspectos negativos, como a utilização de dados pessoais dos indivíduos, por pessoas, empresas e terceiros em colaboração. Nesse contexto, uma análise dos comportamentos de pessoas ligadas a tecnologia da informação, frente ao uso de dados de terceiros sem autorização ou consentimento para benefício próprio em situações supostas faz se necessário. É preciso cuidado com o uso das informações que são armazenadas e organizadas pelos diversos sistemas disponíveis e a ética tem papel fundamental.

Palavras-chave: Segurança de dados; Tecnologia da Informação; Ética profissional.

INTRODUÇÃO

Com o avanço tecnológico há o desenvolvimento de novas ferramentas, entre elas, a internet, que pode ser considerada o meio de comunicação com maior avanço. A informatização de diversas atividades, transforma a Tecnologia da Informação (TI) em uma área cada vez mais relevante expandindo para diversos setores como economia, saúde, jurídico entre outros (REZENDE, 2000; DE SANT'ANNA et al. 2011; SANTOS et al. 2017).

¹ Discente do 8º termo do curso de Sistemas de Informação do Centro Universitário Antonio Eufrásio de Toledo de Presidente Prudente. guilhermeroma@toledoprudente.edu.br

² Docente do curso de Sistemas de Informação do Centro Universitário Antonio Eufrásio de Toledo de Presidente Prudente. Mestre em Ciências Cartográficas pela Universidade Estadual Paulista Júlio de Mesquita Filho. paula_langhi@toledoprudente.edu.br Orientadora do trabalho.

O mercado de TI é um destes que se mantem em expansão devido a constantes atualizações de seus produtos e serviços, assim, os profissionais que atuam nessa área são considerados estratégicos e contribuem para que empresas e pessoas possam enfrentar crises, além de contribuírem para a inovação tecnológica (RIBEIRO; GUIMARÃES; JUNIOR, 2017).

No entanto, a era da informação também trouxe aspectos negativos, como a utilização de dados pessoais dos indivíduos, por pessoas, empresas e terceiros em colaboração, por exemplo, quando um usuário compartilha seus dados em dispositivos de armazenamento em nuvem, por isso, a necessidade do consentimento na coleta e uso de dados ganhou importância para garantir que as pessoas tenham conhecimento da possível utilização de seus dados assegurando sua liberdade e privacidade (HUSSAIN et al. 2020).

A Lei 12.965, conhecida como Marco Civil da Internet, prevê a privacidade como um dos princípios conforme seu artigo 3º, inciso II e determina, ainda, que o fornecimento de dados pessoais a terceiros é vedado, excepcionando-se o caso do fornecimento com o consentimento livre, expresso e informado (BRASIL, 2014). Em agosto de 2018, foi sancionada ainda, a Lei nº 13.709 conhecida como Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em Agosto de 2020. Tratando como “dados pessoais” todas as informações relacionadas a pessoal natural, a LGPD visa normatizar e regular como devem ser tratados os dados coletados dos cidadãos tendo como objetivo defender os dados dos usuários por meio de penalidades significativas caso não haja o cumprimento da mesma, pois (BRASIL, 2018).

Neste contexto, a ética dos profissionais da tecnologia da informação estará sempre à prova, não somente pelo sigilo das informações, uma vez que, dados digitais têm um valor expressivo, portanto, segurança e privacidade tornam-se essenciais. A Ética baseia-se numa filosofia de valores compatíveis com a natureza e o fim de todo ser humano, por isso, “o agir” da pessoa está condicionado a duas premissas consideradas básicas pela Ética: “o que é” o homem e “para que vive”, logo, toda capacitação científica ou técnica precisa estar em conexão com os princípios essenciais da Ética (MOTTA, 1984 – p.69).

Sendo assim, o objetivo deste artigo é descrever quais os comportamentos de pessoas ligadas à tecnologia da informação ou não, frente ao

uso de dados de terceiros sem autorização ou consentimento para benefício próprio em situações supostas.

MATERIAIS E MÉTODOS

O presente trabalho foi desenvolvido em forma de pesquisa quantitativa, descritiva exploratória, através da aplicação de questionário estruturado. O questionário estruturado foi elaborado utilizando a plataforma *online Google Forms* contendo quatro perguntas que abordavam situações supostas que envolvessem os dilemas morais e éticos profissionais a respeito do uso de dados confidenciais de uma empresa na qual a pessoa teria acesso por conta de seu cargo e quais seriam os seus comportamentos. Esses dados incluíam o cadastro de clientes, funcionários/colaboradores e fornecedores, além de informações sobre o endereço, número telefônico, e-mail, dados financeiros, data nascimento, entre outras.

Neste contexto o participante era apresentado as seguintes perguntas:

- Pergunta 1: *“Caso você quisesse sair dessa empresa e quisesse iniciar um empreendimento (Podendo esse empreendimento até mesmo concorrer com a empresa atual que você trabalha). Você, por meio de uma cópia de dados, usaria esses dados para ajudar a estruturar seu negócio? Seja para marketing/divulgação, etc?”*
- Pergunta 2: *“Se caso você fosse mandado embora da empresa, você, por meio de uma cópia de dados, tentaria obter dados para talvez utiliza-los para fins próprios?”*
- Pergunta 3: *“Se caso você fosse pressionado por um superior a copiar os dados e fornecer a ele para um provável uso pessoal dele, você faria?”*
- Pergunta 4: *“Qual seu posicionamento sobre tais atos nas situações a cima?”*

O questionário foi disponibilizado através da *internet* para que os participantes pudessem responder as perguntas.

O convite para participação e o questionário foram direcionados para pessoas do círculo social dos pesquisadores que se disponibilizaram a responder em caráter anônimo onde previamente as perguntas foram explicitadas, através de redes sociais e aplicativos de mensagens. A coleta de dados ocorreu no mês de novembro de 2019 e contou com 43 participantes. Os dados coletados foram lançados no *software* Excel onde foram analisados em porcentagem de acordo com as respostas.

RESULTADOS

A Tabela 1 mostra que, dos 43 participantes, a maioria (60,5%) optaria por não utilizar dados da empresa fictícia em benefício próprio caso desejassem iniciar um novo empreendimento mesmo que fossem pressionadas por um superior.

Ainda sobre os 43 participantes, conforme a Tabela 1, 86% não optaria pelo uso de dados mesmo que não houvesse mais compromisso com a empresa.

Em outra situação, de acordo com a Tabela 1, 60,5% dos participantes acreditam que as situações supostas descritas são incorretas, por tanto, não deve ser praticadas, enquanto que 39,5% acreditam que se não houver prejuízos para empresa e outras partes, não há problemas ao fazer uso dos dados.

Tabela 1 - Uso de dados de terceiros sem autorização ou consentimento para benefício próprio em situações supostas – Presidente Prudente – SP, 2019.

Pergunta 1	Sim	16,3%
	Não	60,5%
	Talvez	23,3%
Pergunta 2	Sim	14,0%
	Não	86,0%
Pergunta 3	Sim, Prontamente	0,0%
	Não, de forma alguma	39,5%

	Talvez, tentaria entender o motivo, mas acabaria fazendo	14,0%
	Talvez, tentaria entender o motivo, mas não faria	41,9%
Pergunta 4	São incorretos, a pessoa não deve fazer isso	60,5%
	Não vejo problema algum, os dados estão ali, é uma cópia, não vai apagar nada da empresa.	0,0%
	Parcial. Se não vai prejudicar ninguém nem a empresa, não há problemas	39,5%

Fonte: Próprio autor

Frente as situações supostas, a maioria dos participantes optaria por não utilizar dados sem autorização e consentimento, mesmo que pressionados por superiores e defendem essas atitudes serem incoerentes com a prática profissional.

A informação é um patrimônio que possui valor, pois se trata de um conjunto organizado e classificado de dados que podem ser consultados e utilizados, dessa forma, a tecnologia da informação tem papel fundamental.

A importância da tecnologia da informação nas empresas hoje é muito clara, a questão a ser abordada agora é a ética nesta função, conforme Pressman (2016) “Ser cuidadoso em usar somente dados precisos, obtidos por meios éticos e legais e usá-los de maneira autorizada”.

Atualmente os profissionais de TI não possuem como em outras profissões um código de ética desenvolvido. Algumas empresas desenvolvem internamente seus próprios códigos, normas ou políticas. Desta forma, a conduta do prestador de serviços é ponto essencial, visto que, caso este profissional falhe na operação de um determinado trabalho ou utilize de informações para bem próprio corre-se o risco

de expor conteúdos sigilosos, levando a inúmeros problemas para os contratantes, bem como para sua credibilidade (MELO; SOUZA; FURTADO, 2014).

Uma menor parte dos participantes responderam que optariam pela utilização dos dados e que essa condição se repetiria em casos de pressão superior. Vale destacar que a ética e a moral são elementos pertencentes a vida da sociedade, faz parte da evolução histórica e altera-se com o passar do tempo. Dessa forma, segundo o autor Abbagnano (1998) a moral é o objetivo da ética, conduta, dirigida ou disciplinada por normas. Para Nalini (1999) a moral é vista como o produto da ética e o conjunto de regras de comportamento e formas de ??? através das quais o homem tende a realizar o valor do bem.

Portanto, a ética e a moral caminham juntas na construção de uma sociedade que visa o bem comum. Olhando para a área da tecnologia, mesmo com a evolução da segurança da informação, ainda existem problemas de invasões às redes diariamente, contudo é importante salientar que estes são atos que ferem a ética e a moral e são conhecidos como crimes cibernéticos e podem ser praticados por profissionais do uso da tecnologia que utilizam seus conhecimentos ou outras pessoas que não sejam da área da TI, de forma ilícita em busca do bem próprio (MELO; SOUZA; FURTADO, 2014).

Faz-se necessário, então, iniciar a regulação das condutas exercidas por profissionais da TI, criando-se códigos de ética similares aqueles existentes em outras áreas do conhecimento como o da saúde, por exemplo. Segundo Masiero (2000), a administração dos sistemas computacionais que oferecem serviços de acesso à Internet, como os provedores da Internet, é normalmente administrada pelos profissionais da informática. Nesse exercício, eles atuam como intermediários entre os provedores de conteúdo e os consumidores, assim, espera-se que estejam capacitados para a adoção de comportamento profissional que dificulte a propagação de condutas que ferem a ética.

Alguns participantes acreditam que caso não houvessem prejuízos para a empresa fictícia ou para os clientes não haveria problemas éticos com relação a tais práticas. É importante reforçar que, os crimes digitais são cometidos por meio do uso de equipamentos eletrônicos como smartphones e computadores, estes, atingem as redes sociais e outras ferramentas disponíveis no espaço virtual, o fato é, que, crimes como estes, são desencadeados por elementos da sociedade que utilizam da tecnologia sem a responsabilidade moral e ética para o bem próprio

ou simplesmente para prejudicar pessoas (VIANNA, 2000). Desta forma, a preocupação com a ética dos profissionais de tecnologia é de suma importância e este deve ser muito transparente com a sociedade, uma vez que, o crescimento da tecnologia envolve informações valiosas (MAISERO, 2000; MELO; SOUZA; FURTADO, 2014),.

A primeira lei que trata de crimes cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, foi a que tipificou atos como invadir computadores, roubar senhas, violar dados de usuários e divulgar informações privada (BRASIL, 2012). O Marco Civil da Internet (Lei 12.965/2014) foi sancionado em 2014 e regula os direitos e deveres dos internautas, ele protege os dados pessoais e a privacidade dos usuários, assim, somente mediante ordem judicial pode haver quebra de dados e informações particulares existentes em sites ou redes sociais (BRASIL, 2014).

Na América Latina, o Brasil é um dos países com a regulamentação mais atrasada. A Lei Geral de Proteção de Dados, mais conhecida pela sua sigla LGPD (Lei 13.709/2018), que entrou em vigor em Agosto de 2020, chegou para fixar parâmetros do mesmo tema da lei europeia. Para as organizações brasileiras, é preciso se adequar a uma nova realidade de segurança de informação, conhecer a legislação sobre consentimentos e transparência que fara parte do dia a dia.

Para reduzir ameaças e/ou crimes, encontramos diversas barreiras, pois administrar a segurança geralmente é um grande problema. Segundo Campana (1997, p 1) “segurança não acarreta novos programas, novas facilidades e, principalmente, não é um tópico importante para a gerência das empresas, pois segurança não gera receita”. Quanto menos protegermos as informações maior o impacto nos negócios e ativos.

Todas as formas de proteção devem diminuir as ameaças ou pelo menos os impactos das mesmas, dessa forma, inserir uma política de segurança é essencial na gestão da segurança da informação. Uma política de segurança pode ser definida como instruções que orientam os comportamentos dos empregados para proteger informações e é um elemento fundamental de segurança (NEVES, 2015).

O objetivo de um programa de conscientização de segurança é a comunicação da importância das políticas de segurança e os danos que as falhas do não cumprimento dessas regras podem causar. Dada a natureza humana, os empregados as vezes ignoram ou sabotam as políticas que parecem ser

injustificadas ou que demandam muito tempo, a gerência tem a responsabilidade e o dever de garantir que empregados compreendam a importância das políticas e sejam motivados para atendê-las (MELO; SOUZA; FURTADO, 2014; NEVES, 2015).

O maior objetivo da implementação de uma política de gestão da segurança de informações não é garantir total segurança e sim controlar os riscos, para que eles não sejam ameaças para as empresas e que caso aconteçam, possam acarretar em menor impacto nos negócios (NETTO; SILVEIRA, 2017).

CONCLUSÃO

Esta pesquisa teve como objetivo descrever quais os possíveis comportamentos de pessoas ligadas à tecnologia da informação ou não, frente ao uso de dados de terceiros sem autorização ou consentimento para benefício próprio em situações supostas. A maioria dos participantes optariam pela não utilização desses dados mesmo em situações de pressão de superiores considerando tais condutas incorretas. Uma quantidade menor optaria pelo uso em determinadas situações como em casos de demissão ou caso não houvessem consequências.

A tecnologia é parte integrante da sociedade, e o uso de suas diversas abordagens é essencial ao desenvolvimento humano, no entanto é preciso cuidado com o uso das informações que são armazenadas e organizadas pelos diversos sistemas disponíveis. Cabe ressaltar que o profissionalismo e ética do profissional envolvido com a área de tecnologia é de suma importância, visto que este possui o conhecimento, bem como o acesso a todo o compilado de informações. Informações estas que, no mundo competitivo que estamos inseridos, tornam-se alvos de ataques, bem como do uso indevido, para que possam alcançar o bem próprio ou até mesmo prejudicar algo ou alguém. Desta forma, o conceito de ética para utilização da tecnologia de forma consciente e em busca do bem maior para a sociedade é ponto crucial.

REFERÊNCIAS

ABBAGNANO, Nicola. **Dicionário de filosofia**. 4. ed. São Paulo: Martins Fontes, 2000.

BRASIL, **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário oficial da União, Brasília, DF, 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 06 nov. 2019.

BRASIL, **Lei 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (marco Civil da Internet). Diário Oficial da União, Brasília, DF, 14 de agosto de 2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 07 nov. 2019.

CAMPANA, Carlos. Segurança: Você se preocupa com isso? **News Generation**. V1.n.1.,p 1-3. São Paulo, 30 mai. 1997. Disponível em: <<http://www.rnp.br/newsgen/9705/n1-3.html>>. Acesso em: 05 nov. 2004.

HUSSAIN, Ali et al. Performance and Security Challenges Digital Rights Management (DRM) Approaches Using Fog Computing for Data Provenance: A Survey. **Journal of Medical Imaging and Health Informatics**, v. 10, n. 10, p. 2404-2420, 2020.

MAISERO, Paulo Cesar. **Ética em Computação**, Editora USP, São Paulo, 2000.

MELO, Ronaldo Oliveira; DE SOUZA, Roniérisson Soalheiro; FURTADO, Maria Renata Silva. Ética e o Profissional de Tecnologia da Informação. **Revista Pensar Tecnologia**, v. 3, n. 2, 2014.

NALINI, José Renato. **Ética geral e profissional**. 3 ed. São Paulo: Revista dos Tribunais, 2001.

NEVES, Leonel Santos. **Segurança da Informação nas Empresas e Organizações**. Manografia. Rio de Janeiro, 2015.

PRESSMAN, Roger; MAXIM, Bruce. **Engenharia de Software-8ª Edição**. McGraw Hill Brasil, 2016.

REZENDE, Ana Paula de. Centro de informação jurídica eletrônico e virtual. **Ciência da informação**, v. 29, n. 1, p. 51-60, 2000.

RIBEIRO, Guilherme Fernandes; GUIMARÃES, Leila Jane Brum Lage Sena; JÚNIOR, André Luiz Moura. MERCADO DE TECNOLOGIA DA INFORMAÇÃO: DEMANDAS PROFISSIONAIS. **REVISTA DE TRABALHOS ACADÊMICOS-UNIVERSO BELO HORIZONTE**, v. 1, n. 2, 2017.

SANT'ANNA, Paulo Roberto de et al. Tecnologia da informação como ferramenta para a análise econômica e financeira em apoio à tomada de decisão para as micro e pequenas empresas. **Revista de Administração Pública**, v. 45, n. 5, p. 1589-1611, 2011.

SANTOS, Alaneir de Fátima dos et al. Incorporação de Tecnologias de Informação e Comunicação e qualidade na atenção básica em saúde no Brasil. **Cadernos de Saúde Pública**, v. 33, p. e00172815, 2017.

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, n. 3, p. 375-397, 2007.

VIANNA, Túlio Lima. Dos crimes pela internet. **Revista do CAAP**, p. 367-385, 2000.