Anotações do artigo intitulado “Segurança e privacidade dos dados no mundo hiperconectado”:

1º parágrafo: O avanço tecnológico resultou em uma sociedade conectada a todo momento através de dispositivo capazes manipular um grande volume de dados. Com a evolução surgiu grandes oportunidades e facilidades para todos.

2º parágrafo: A internet das coisas que nos possibilita integrar o mundo real e virtual, fazendo com que se permaneça em constante comunicação. Dispositivo com tecnologia IoT são capazes de desempenhar tarefas se a necessidade de interação humana.

3º parágrafo: No mundo atual em que vivemos, diversos dispositivos que se auto comunicam e através da coleta e manipulação de dados controlam nosso dia a dia. Esses dados são compartilhados de maneira contínua com diversos servidores onde se é realizado a manipulação de dados a fim de extrair informações relevantes.

4º parágrafo: Devido às características desses softwares eles resultam vários problemas como vazamento de dados realizado de maneira simples por hackers, até mesmo dispositivos mais avançados com sistema mais bem desenvolvido ficam expostos. Em 2020, um ataque cibernético de grande escala atingiu milhares de organizações, das quais dessas organizações abrangem agências governamentais dos EUA.

5º parágrafo: Em 2013, após o vazamento de informações confidenciais de um programa de espionagem de cidadãos de diversos países, a questão da proteção de dados ganhou destaque sendo aprovado um projeto intitulado “O Direito à Privacidade na Era Digital”, apresentado pela Alemanha e Brasil. O Brasil sancionou outras medidas relacionadas à privacidade, como Marco Civil e LGBD, que especificam como os dados dos cidadãos devem ser tratados. A GPDR estabelece as regras relativas à proteção, tratamento e livre circulação de dados pessoais de pessoas nos países da União Europeia.

6º parágrafo: Devido ao monitoramento átomo de dados, o problema é agravante, pois os dispositivos IoT são vulneráveis ​​e têm limitações com isso a exposição de dados é recorrente. Os smartphones que carregamos conosco o tempo todo são exemplos de IoT, coletando e transmitindo constantemente uma série de dados sobre nós e nossos hábitos. Se esses dados forem expostos, podem levar a sérios problemas para o usuário. Através de violações de segurança nos sistemas e a inocência do usuário são o principal método de coleta de dados, essa ação é realizada com a intenção de obter algum benefício como lucro com venda de informações, extorsão ou demandas políticas.

7º parágrafo: A imprescindibilidade de se construir soluções para preservar privacidade e segurança se tornou essencial. Em 2018, o impacto da comercialização e divulgação abusiva de dados privados causou um custo global médio de US$ 3,86 milhões. O Brasil está entre os países com mais violações de dados em 43%, a média global é de 27%. De acordo com dados de 2021, 98% dos dispositivos IoT não possuem criptografia de tráfego e 57% desses dispositivos possuem vulnerabilidades.

8º parágrafo: As ações realizas pelo governo despertaram um maior interesse da população em segurança e privacidade na era digital. O Plano Nacional da Internet das Coisas e o Marco Civil da Internet são exemplo de medidas que mostram a relevância do assunto. Embora tenham sido lançadas iniciativas para regular e fortalecer a proteção de dados, há uma clara necessidade de soluções técnicas que entendam as caracteristicas da IoT e evitem o vazamento de informações.

9º parágrafo: O principal objetivo deste artigo é destacar o quão importante é para a sociedade atentar para essas questões de privacidade e segurança nesse contexto de hiperconectividade que estamos enfrentando.