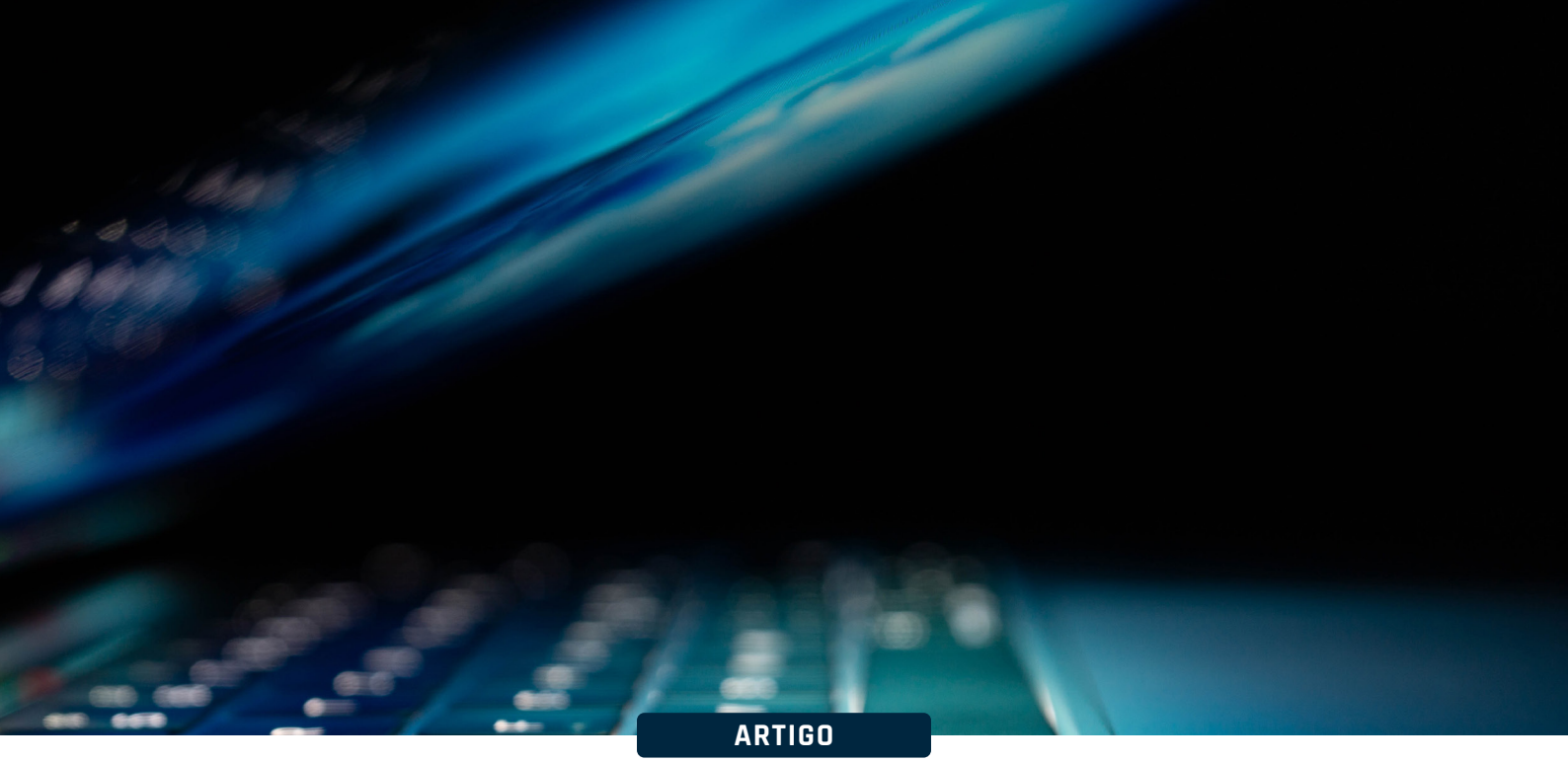

ARTIGO

SEGURANÇA E PRIVACIDADE DOS DADOS NO MUNDO HIPERCONECTADO

POR
Michele Nogueira
michele@dcc.ufmg.br

A evolução tecnológica em *hardware* e *software* culminou no surgimento e na popularização de dispositivos computacionais capazes de coletar, armazenar e processar, de forma eficiente e transparente, um grande volume de dados heterogêneos. Vivemos em um mundo hiperconectado em que, através de seus diferentes dispositivos computacionais e da Internet, as pessoas permanecem continuamente conectadas nas ruas, em suas casas, no trabalho e na escola. Isso tem resultado em transformações na sociedade e inovação aceleradas, gerando facilidades e grandes oportunidades para pessoas e instituições. .

A Internet das Coisas (do inglês, *Internet of Things* - IoT) é associada como um facilitador na coleta desses dados e vem potencializando a revolução para a era digital. Os dispositivos IoT inter conectam-se para desempenhar atividades sem a necessidade da intervenção humana. Estas atividades suportam aplicações relevantes e, muitas vezes, sensíveis, tais como o monitoramento à distância da saúde, do trânsito, a automação de atividades industriais, entre outros. Um exemplo de sua relevância consiste na criação do fundo de investimento para o desenvolvimento da IoT no Brasil, lançado em parceria entre o Ministério da Ciência, Tecnologia

e Inovação (MCTI), o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e a empresa Qualcomm Ventures [1][2].

Nesse contexto de mundo hiperconectado, os dispositivos monitoram o dia a dia dos seus usuários através da coleta de dados e sua transmissão pela Internet. Estes dispositivos, de baixa capacidade computacional e alimentação energética limitada, englobam sensores vestíveis (implantados ou sobre o corpo humano), equipamentos domésticos, telefones móveis inteligentes (*smartphones*), câmeras IP e outros. Eles conectam-se continuamente a servidores responsáveis pelo processamento e análise dos dados a fim de extrair informações através de correlações e inferências. Eles também são capazes de se comunicarem entre si através da comunicação sem fio, orquestrada por protocolos e padrões.

Estas características levam a problemas como vazamentos de informação a partir de ações simples realizadas por atacantes, como o monitoramento do tráfego da rede, mesmo em um tráfego criptografado. Assim, o uso de protocolos da Internet tradicional, os quais foram projetados para dispositivos mais robustos e com conexões confiáveis, se torna ineficiente na maioria dos cenários IoT. As características citadas somadas à diversidade e à quantidade de dispositivos IoT resultam em um grande volume de dados, como aqueles sensíveis e relacionados à saúde e à segurança dos usuários, requerendo um alto nível de privacidade. Em 2020, milhares de organizações que operam com dispositivos IoT foram infectadas no escopo do ataque contra a SolarWinds, sendo que dentre essas organizações encontram-se agências governamentais dos Estados Unidos [3]. O conceito de segurança na Internet pode ser considerado recente e, infelizmente, a segurança no projeto dos dispositivos não acompanhou o ritmo acelerado da inovação, levando a dispositivos com várias brechas e vulnerabilidades de segurança. A IoT é mais suscetível a ataques do que a Internet tradicional devido ao meio de comunicação sem fio, às vulnerabilidades legadas e às limitações de recursos dos dispositivos. Entretanto, as novas aplicações e serviços viabilizados pela IoT não deveriam representar um risco aos direitos de segurança e privacidade dos usuários, exigindo soluções eficientes.

Nos últimos anos, a privacidade na era digital ganhou a atenção das principais organizações do mundo, como da Organização das Nações Unidas (ONU) e da União Européia (UE). Este fato foi motivado pelo caso Snowden de 2013, um ex-agente da Agência Central de Inteligência (do inglês, *Central Intelligence Agency* - CIA) dos EUA que vazou informações sigilosas do país sobre programas de vigilância utilizados para espionar a população americana e de outros países, entre eles o Brasil. No mesmo ano, a ONU aprovou o projeto "O direito à privacidade na era digital", apresentado pelo Brasil e Alemanha. O

Brasil tomou posições ainda mais críticas, através da "Lei Geral de Proteção de Dados" (LGPD) e o "Marco Civil da Internet" que, respectivamente, sancionam uma série de normas sobre a privacidade dos usuários de provedores de serviços e aplicações da Internet. A UE avançou nesse sentido, criando o Regulamento Geral sobre a Proteção de Dados (GPDR), detalhando em lei as diretrizes e regras para proteger os dados dos seus cidadãos. Desta forma, as empresas, tais como os provedores de serviço, que apresentarem irregularidades estão sujeitas a multas. Estes fatos evidenciam a necessidade de medidas de privacidade na era digital.

O problema de privacidade na IoT se agrava, pois os dispositivos monitoram de forma autônoma dados privados, muitas vezes sensíveis, sobre a rotina dos usuários. Diante das vulnerabilidades e das limitações dos dispositivos da IoT, o vazamento de dados e de informações é recorrente. Um *smartphone* é um bom exemplo de um dispositivo IoT que coleta e transmite dados privados sobre seus usuários pela Internet. No geral, estes dispositivos são controlados por sistemas operacionais que por padrão proveem serviços de localização através da Internet. No entanto, os dados trafegados pelos dispositivos da IoT, se capturados e interpretados, expõem seus usuários a problemas sérios de privacidade e segurança pessoal. A principal forma de capturar estes dados privados é através de ataques que exploram a inocência dos usuários e as brechas de segurança nos sistemas de computação e comunicação. Estes dados são adquiridos com o objetivo de lucrar com a venda de informações, com chantagens ou apelos políticos. Este fato está evidenciado e detalhado na matéria de capa intitulada "*Broadbandits: The surging cyberthreat from spies and crooks*", edição de 19 de Junho de 2021, da revista "The Economist".

Ao longo dos anos, torna-se cada vez mais evidente a necessidade de projetar soluções de segurança e privacidade para a IoT e para este cenário de hiperconectividade. Em 2018, os impactos da comercialização e da divulgação indevida de dados privados representaram um custo médio global de 3,86 milhões de dólares americanos. Além disso, o Brasil apresenta uma das maiores taxas de risco de violação de dados com 43%, comparados a 27% da média global [4]. Pesquisas realizadas em 2021 indicam que não existe criptografia no tráfego em 98% dos dispositivos IoT e que 57% destes dispositivos apresentam vulnerabilidades médias ou severas [5].

As iniciativas governamentais despertaram um maior interesse da população em segurança e privacidade na era digital. O Plano Nacional de Internet das Coisas [1] estuda os impactos da IoT na sociedade brasileira e incentiva a criação de sistemas de segurança na IoT. Isto, aliado ao Marco Civil da Internet, determina como as empresas provedoras de Internet e de serviços devem tratar os dados de acesso e navegação dos usuários. O Plano Nacional da Internet das Coisas e o Marco Civil da Internet demonstram a relevância do assunto e o incentivo no desenvolvimento de soluções de segurança relacionadas ao controle e gestão de dados privados. O Marco Civil foca ainda na neutralidade

da Internet, ou seja, as empresas que fornecem a conexão não devem ter acesso aos conteúdos acessados pelos usuários. Os principais alvos destas medidas de segurança são empresas que se aproveitavam das brechas na lei para comercializar os dados de acesso e navegação dos clientes. Entretanto, apesar das iniciativas dos órgãos públicos para normatizar e reforçar a defesa pelo direito de privacidade, é evidente a necessidade de soluções técnicas que compreendam as características específicas da IoT e que previnam o vazamento de informação.

Assim, finalizo este artigo com um convite para que se unam a nossa comissão especial de Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação na prevenção da privacidade dos dados e segurança dos nossos sistemas digitais. Este artigo tem como principal objetivo ressaltar a importância para a sociedade de nos atentarmos para essas questões de privacidade e de segurança nesse contexto de hiperconexão em que nos deparamos. Se ficou interessado em entender mais sobre o tema e gostaria de contribuir de alguma forma com a área de segurança da informação e de sistemas computacionais, entre em contato comigo.

Referências

1. Plano Nacional de Internet das Coisas (IoT). Diário Oficial da União (DOU), o Decreto no 9.854, de 25 de junho de 2019.
2. MCTIC, BNDES e QUALCOMM: Fundo de Investimentos para IoT. Último acesso: 20 de junho de 2021.
3. Lucian CONSTANTIN. SolarWinds attack explained: And why it was so hard to detect. publicado em dezembro de 2020. Último acesso: 21 de junho de 2021.
4. 2020 Cost of a Data Breach Report. Último acesso: 20 de junho de 2021.
5. OT/IoT Security Report. Último acesso: 20 de junho de 2021.

MICHELE NOGUEIRA é Cientista da Computação atuando na área de redes de computadores e segurança de redes. Possui doutorado em Ciência da Computação pela Sorbonne Université - UPMC/LIP6, França (2009) e realizou Pós-doutorado na Universidade Carnegie Mellon (CMU), EUA. É professora associada do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), membro sênior da Association for Computing Machinery (ACM) e do Institute of Electrical and Electronics Engineers (IEEE). É coordenadora da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (SBC) e é a primeira mulher a coordenar o Comitê Técnico da Internet da IEEE Communications Society (EUA). É líder do Centro de Ciência de Segurança Computacional e coordena o projeto temático MCTIC/FAPESP MENTORED, cujo um dos objetivos é criar um ambiente experimental acadêmico para Cibersegurança em parceria com a Rede Nacional de Ensino e Pesquisa (RNP).