BREVE COMENTÁRIO SOBRE A INTERNET DAS COISAS A LUZ DO DIREITO PENAL BRASILEIRO
BRIEF COMMENT ON THE INTERNET OF THINGS UNDER BRAZILIAN CRIMINAL LAW

Claudio Joel Brito Lóssio[1] | *Coriolano Aurélio Almeida Camargo Santos*[2]

Resumo: A sociedade atual onde vivemos está sendo tomada por uma nova sociedade digital, onde praticamente todas as relações entre pessoas e máquinas estão voltadas para a comunicação via internet, e essa situação dá vez a IoT (Internet of Things). Todo esse processo é uma transformação social que traz a sociedade a quo para um novo status, a ad quem, na sociedade digital. A IOT é a sigla da Internet of Things, traduzindo para o português, Internet das Coisas, terminologia voltada para todos os computadores, máquinas, dispositivos, equipamentos que possuam chip de processamento e acesso a internet, que possa interagir com seres humanos com a finalidade de proporcionar uma maior eficiência e comodidade na vida de todos. Os riscos de ter esses dispositivos violados por terceiros mal-intencionados podem dar acesso a dados privados do proprietário, podendo ser de amplitude cruel ou até mesmo catastrófica. Uma breve abordagem relacionando a IoT ao Direito Penal Brasileiro será apresentada na forma relacional entre alguns artigos legais e riscos do IoT, assim como medidas preventivas para que seja minimizada a incidência de violação ilegal dos dispositivos IoT, para que se permita uma maior cognição acerca desta nova seara.

Palavras-Chave: Sociedade Digital. Internet das Coisas (IoT). Direito Penal Brasileiro, Direito das Máquinas.

***Abstract**: The current society in which we live is being taken over by a new digital society, where practically all people and machines relationships are on communication via the internet, and this situation gives rise to IoT (Internet of Things). This process is a social transformation that brings society a quo status for a new status, the ad quem, in the digital society. IOT is the acronym of Internet of Things, translating into Portuguese, Internet das Coisas, terminology aimed at all computers, machines, devices, equipment that have processing chip and internet access, that can interact with humans for the purpose to provide greater efficiency and convenience in everyone's life. The risks of having these devices violated by malicious third parties may give access to private data of the owner and may be cruel or even catastrophic. A brief approach linking IoT to Brazilian Criminal Law will be presented in relational form between some legal articles and IoT risks, as well as preventive measures to minimize the incidence of illegal IOT violations, to allow a greater cognition about this new crop.*

***Keywords**: Digital Society. Internet of Things (IoT). Brazilian Criminal Law, Law of machines.*

---

1 Mestrando em Ciências Jurídicas pela UAL - Universidade Autônoma de Lisboa-Portugal; Pós-Graduando em Direito Digital & Compliance pela Damásio Educacional, Pós-Graduando em Direito Penal e Criminologia pela URCA - Universidade Regional do Cariri, Pós-Graduando em Direito Notarial e Registral pela Damásio Educacional, Pós-Graduando no MBA Executive em Gestão de TI pela FACEAR - Faculdade Educacional Araucária. (2017). Membro da Coordenadoria de Pesquisa de Tecnologias Disruptivas da OAB/SP. Membro da Comissão de Direito Digital e Compliance da OAB/SP. Advogado. Palestrante. Professor. Email: claudiojoel@juscibernetica.com.

2 Ph.D. Advogado. Diretor Titular Adjunto do Departamento Jurídico da FIESP. Conselheiro Estadual eleito da OAB/SP (2013/2018). Presidente da Comissão de Direito Digital e Compliance da OAB/SP. Mestre em Direito na Sociedade da Informação e certificação internacional da "The High Technology Crime Investigation Association (HTCIA)". Doutor em Direito com certificado internacional em Direito Digital pela Caldwell Community College and Technical Institute. Professor e coordenador nacional do programa de pós-graduação em Direito Digital e Compliance da Faculdade Damásio. Professor convidado dos cursos de pós-graduação da USP/PECE, Fundação Instituto de Administração, Univeridade Mackenzie, Escola Fazendária do Governo do Estado de São Paulo Fazesp, Acadepol-SP, EMAG e outras. Desde 2005 ocupa o cargo de juiz do Egrégio Tribunal de Impostos e Taxas do Estado de São Paulo. Professor convidado do curso superior de Polícia da Academia de Polícia Civil de São Paulo. Professor da Escola Nacional dos Delegados de Polícia Federal - EADELTA.

1 INTRODUÇÃO

O meio social está cada vez mais envolvido com a era da informática visto que a maioria das atividades seja de entretenimento ou de trabalho estão relacionadas diretamente com a internet, e isto traz uma novo status social, a sociedade digital.

Estamos em tempos onde praticamente todos os dispositivos que se adquire, possui conexão com internet, como também chip para processamento. Casas automatizadas, geladeiras que analisam a quantidade de comida estocada, além da data de validade dos produtos, carros autônomos, smartwatchs, são exemplo de coisas, e estas preservam uma quantidade imensa de informações de seus proprietários.

Conforme citado anteriormente já estamos vivendo tempos em que a sociedade normal está em transito para um novo molde de sociedade, a digital e para tanto em um futuro próximo estaremos assim como os seres humanos são parte de um meio ambiente, também faremos parte de um meio ambiente digital.

No decorrer desta escrita será apresentado no primeiro capítulo o que realmente é esse novo termo que está sendo abordado como objeto de breve apresentação, IoT, Internet of Things ou Internet das Coisas, que, de antemão, já antecipamos o conceito deste como sendo todo equipamento com chip de processamento e internet. Equipamento o qual poderá ser inteligente ao ponto de ajudar a nós humanos e nossas atividades diárias.

No segundo capítulo serão abordados alguns dos riscos que os equipamentos com chip e internet poderão causar aos seres humanos, visto que estes terão acesso a informações relacionadas a vida privada e a intimidade de cada pessoa que interagir consigo. E se estes sofrerem algum tipo de violação por um terceiro não autorizado, este acabará por violar a garantia fundamental do direito a privacidade e a intimidade por exemplo.

Já no terceiro capítulo ocorrerá uma relação do que os equipamentos com chip e internet poderão causar ao terem sua segurança violada por um terceiro não autorizado, e os artigos do Código Penal Brasileiro. Por último serão apresentadas braves medidas de segurança para que reduzam tanto os riscos quando não se criem novas vulnerabilidades nestes equipamentos. Agora iniciaremos com o IoT.

2 O QUE É IOT?

A todo momento na internet surgem novas terminologias que todo mundo vê em cada compartilhamento de Internet, em cada notícia, mas ninguém sabe ao certo o que significa, como por exemplo, temos os termos *Big Data*, *Blockchain*, *Machine Learning*, *Data Mining*, como também a *Internet of Things*.

IoT é a sigla de *Internet of Things*, que traduzindo para o português temos Internet das Coisas, que é a denominação atribuída para dispositivos com chip de processamento e acesso a internet que pode se comunicar com pessoas, máquinas, computadores, animais e objetos sem que seja necessário qualquer tipo de intervenção humana. (COELHO, 2017).[3]

Casas Inteligentes; cidades inteligentes, incluindo controle de acessos, tráfegos, pessoas; controle de água, luz, gás e serviços municipais automatizados; monitoramento da saúde de pessoas por dispositivos médicos com alarme assim como comunicação de dispositivos que monitoram a evolução e os exercícios físicos praticados, para assim o personal trainer e os planos de saúdes assim como o nutricionista acompanhar seu cliente; Todos os produtos não necessitarão de códigos de barras visto que os RFIDs identificarão os produtos e todas as suas características; controle de animais, vacinação automática, colheita; na segurança, a deteção de pessoas através do controle facial, assim como o monitoramen-

3 COELHO, Pedro. Internet das Coisas: Introdução Prática. Lisboa: FCA.2017. p. 02.

to de eventos atípicos fará parte do dia a dia; O RFID proporcionará uma logística de extrema eficácia; Os sapatos, roupas, e acessórios inteligentes também nos completarão. Mas por último, a localização de pessoas e animais através de implantes de chips com internet nos transformará em uma coisa? (COELHO, 2017).[4]

Algumas problemáticas devem ser levantadas para que respostas surjam o mais breve possível quando se fala em violação ilegal dos dispositivos IoT dentro de um âmbito do Direito:

1) Esses dispositivos possuem qualidade suficiente em seus meios de proteção?
2) Qual tipo de criptografia utilizada na comunicação entre dispositivos?
3) O algoritmo contido nesses dispositivos que estão coletando informações é aberto ou fechado?
4) O usuário está de acordo com o que a maneira que a tecnologia do dispositivo tem acesso a sua privacidade?

Essa problemática está sendo apresentada com a maior brevidade possível visto que a Internet das Coisas, utilizam-se de sensores, sistemas operacionais próprios, equipamentos sem controle de qualidade, plataformas de análise de dados que podem ser armazenados em servidores sem qualquer tipo de controle e ou segurança. Cade pelo menos os termos de uso?

A pergunta fundamental, contudo, não é qual a próxima tecnologia, e sim como o Direito lidará com a IoT?

Passamos, portanto, a descrever os riscos que envolvem essas tecnologias.

2.1 RISCOS

O maior risco diante do exposto acerca da IoT está relacionado à violação ao direito a privacidade e a intimidade de seus proprietários certo? Não. A internet das coisas, segundo o exposto anteriormente, não está vinculada de forma exclusiva a forma privada de cada indivíduo em seu ambiente particular. Os equipamentos com chip de processamento ligados a internet estarão também presentes no meio ambiente digital, na sociedade digital, e estando neste novo modelo de sociedade dinâmica consequentemente estará dentro da vida de todos.

Submetendo-se às regras de direito vigentes, inclusive às pedras de toque expressas por Melo (2014)[5], fundamentalmente, o Princípio da supremacia do interesse público e Princípio da indisponibilidade do interesse público. As futuras criações envolvendo IoT deverão se atentar não só no bem estar individual do futuro proprietário de alguma criação, como também na influência, riscos e vulnerabilidades ao coletivo.

Segundo o expresso anterior, além de ficarem submissos aos princípios fundamentais do direito administrativo, há uma real importância de um funcionamento e regulamento de excelência da IoT visto que a privacidade e a intimidade praticamente são direitos constitucionais que podem ser violados facilmente ao conseguir invadir um dispositivo IoT. Mas quando a invasão a um dispositivo IoT acabar por gerar um crime que atentem contra a vida de alguma pessoa diversa do proprietário, por exemplo?

Segundo Coelho (2017)[6], os principais perigos que essa nova roupagem de sociedade com IoT, a digital, poderá causar são:

4 Idem. p. 05.

5 MELLO, Celso Antônico Bandeira de. Curso de Direito Administrativo. 32. ed. São Paulo: Malheiros. 2014. p. 98.

6 COELHO, Pedro. Internet das Coisas. p. 212.

1) Danos Físicos ou estragos materiais, incluindo ferimentos e morte;
2) Redução ou inibição de sistemas de segurança;
3) Danos de Imagem;
4) Perda de Confiança;
5) Indisponibilidade de Serviços;
6) Roubo de Propriedade Intelectual;

Essas acima, são alguns riscos citados, muito embora uma extensão infinita de possibilidades possa ser gerada, e a seguir veremos as situações acima relacionadas ao Código Penal Brasileiro.

A despeito dos bens jurídicos ofendidos nestes casos, um outro fator complicador em relação a essas tecnologias é que as principais práticas que as envolvem em ilícitos, assim como os delitos gerados através da internet, são voltados para o anonimato. O criminoso acredita que a omissão de sua identidade durante suas práticas é perene, e que isso é suficiente para que não responda por seus atos. O raciocínio ganha ares de veracidade se pensarmos na estrutura de segurança pública disponível hoje no Brasil. A busca pela o anonimato é simplesmente a busca da fuga do ato punível visto que o criminoso que busca a internet, e consequentemente, a IoT, para a prática delituosa sabe que este ambiente está fértil para a prática criminosa impune.

Conforme nossa exposição no último tópico, um dos meios para se promover maior segurança e impossibilitando esse tipo de delito, o cibercrime, é através de uma maior rigidez nas políticas de segurança não só em amplitude governamental, mas sim advindo principalmente das empresas que disponibilizam estas tecnologias e dos próprios usuários (UNTERSINGER, 2014)[7].

2.2 IOT E O CÓDIGO PENAL BRASILEIRO

A busca pelo direito para se chegar a justiça é uma garantia constitucional de cada pessoa que compõe um país, e segundo a Constituição Federal do Brasil de 1988, em seu artigo 5: XXXIX – não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

E como ficará definido a violação de um equipamento com internet, visto que, esta "coisa com internet" pode ser considerada um dispositivo informático? Sim, pois a informática é a junção dos termos informação automática, que é o principal fundamento de operação técnico das coisas com internet. Então a violação deste cairia bem para Código Penal Brasileiro no Artigo 152-A[8]:

> **Invasão de Dispositivo Informático**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (grifo nosso)

Diante do exposto, a violação e ou a geração de vício em dispositivos, máquinas, computadores, pessoas que sejam e ou estejam envolvidas na IoT, caberá além de ação cível de dano material e moral, caberá diretamente ação de cunho penal.

Rememorando os itens propostos por Coelho (2017), listamos abaixo os tipos penais no do Código Penal Brasileiro[9] correspondentes mais comuns àquelas práticas arroladas pelo autor.

7 UNDERSINGER, Martin. Anonymat sur Internet. p. 217.

8 CÓDIGO Penal Brasileiro. Decreto-Lei 2.848/1940, de 07 De dezembro. [Em linha]. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html>. Acesso em: 20 set. 2017.

9 CÓDIGO Penal Brasileiro. Decreto-Lei 2.848/1940, de 07 De dezembro. Ibidem.

2.2.1 Danos Físicos ou estragos materiais, incluindo ferimentos e morte

- **Homicídio simples**: Art. 121. Matar alguém;
- **Lesão corporal**: Art. 129. Ofender a integridade corporal ou a saúde de outrem;
- **Dano**: Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia.
- **Incêndio**: Art. 250 - Causar incêndio, expondo a perigo a vida, a integridade física ou o patrimônio de outrem;
- **Perigo de desastre ferroviário**: Art. 260 - Impedir ou perturbar serviço de estrada de ferro;
- **Atentado contra a segurança de transporte marítimo, fluvial ou aéreo**: Art. 261 - Expor a perigo embarcação ou aeronave, própria ou alheia, ou praticar qualquer ato tendente a impedir ou dificultar navegação marítima, fluvial ou aérea;
- **Atentado contra a segurança de outro meio de transporte**: Art. 262 - Expor a perigo outro meio de transporte público, impedir-lhe ou dificultar-lhe o funcionamento.
- **Epidemia**: Art. 267 - Causar epidemia, mediante a propagação de germes patogênicos.

2.2.2 Redução ou inibição de sistemas de segurança

- **Violação de domicílio**: Art. 150 - Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências.

2.2.3 Danos de Imagem

- **Difamação:** Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação;
- **Injúria:** Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.

2.2.4 Perda de Confiança

- **Violação de correspondência**: Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem;
- **Divulgação de segredo**: Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem.

2.2.5 Indisponibilidade de Serviços

- **Furto:** Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel;
- **Extorsão indireta:** Art. 160 - Exigir ou receber, como garantia de dívida, abusando da situação de alguém, documento que pode dar causa a procedimento criminal contra a vítima ou contra terceiro;
- **Apropriação indébita:** Art. 168 - Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção;
- **Estelionato:** Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento;
- **Atentado contra a segurança de serviço de utilidade pública**: Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública;

- **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**: Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.

2.3 ROUBO DE PROPRIEDADE INTELECTUAL

Violação de direito autoral: Art. 184. Violar direitos de autor e os que lhe são conexos.

Diante de todos os tipos penais expostos acima, alguns podem estar se perguntando, como a IoT poderá influenciar para se chegar a todos esses crimes. Pois é, a invasão dessas coisas com internet é o meio para se chegar a qualquer delito citado anteriormente. Mas alguns ainda podem estar se perguntando como a IoT poderá causar uma Epidemia? É muito simples, imagine que em um determinado laboratório, o local onde um vírus que esteja em quarentena para estudo para a criação de uma vacina seja completamente controlado pela internet, onde apenas máquinas poderão manusear esse vírus e um determinado *Cracker*[10] invade o sistema de controle desse laboratório e tem acesso a essas máquinas. Poderão realmente fazer o que quiser, não é? Inclusive deixar esse tal vírus em contato com pessoas desse local. Parece coisa de filme, mas tal realidade pode não estar tão distante. (UNTERSINGER, 2014).[11]

O principal fator que proporcionará violação destes dispositivos será o usuário, visto que a falta de perícia, imprudência ou negligência causada por este é o que normalmente abre as portas para que pessoas com finalidade delituosa tenha acesso aos equipamentos com internet.

Veremos a seguir mais detalhes acerca de algumas medidas de segurança que proporcionam maior risco e abrindo novas vulnerabilidades em redes com equipamentos com internet.

2.4 MEDIDAS DE SEGURANÇAS BÁSICAS

Como citado, o ponto mais fraco que pode gerar danos em uma estrutura de segurança é o próprio usuário, pois comumente este acredita que não será invadido, e assim faz com que não busque se aperfeiçoar em medidas básicas se segurança da informação, ou continue no modo imprudente e negligente de se operar os equipamentos com chip e internet.

Veja o seguinte exemplo, onde um usuário pode ter seu dispositivo com a segurança violada ao se conectar em uma rede sem fio, como a que que vários estabelecimentos comerciais oferecem. Segundo uma das maiores empresas em segurança da informação do mundo, a Kaspersky [12]:

> As redes sem fio são muitas vezes inseguras e são paraísos para os cibercriminosos que que andam em cafés, hotéis restaurantes e muitos outros lugares com acesso público a Internet e que buscam roubar o mais possível for de informações financeiras e pessoais.

Assim, ao ter seu dispositivo violado ao acessar uma rede sem fio sem segurança e posteriormente se conectar na rede de sua casa e ou de sua empresa poderá estar permitindo que o hacker que obteve a violação do dipositivo do usuário, consiga acesso aos equipamentos desta nova rede, seja computador, smartphone, ou equipamentos com chip e internet.

---

10 Crime Hacker, Cracker. Quebrador: É a pessoa que detém vasto conhecimento em informática, e o utiliza com fins ilícitos.

11 UNDERSINGER, Martin. Anonymat sur Internet. p. 202.

12 Kaspersky. Como Evitar uma rede wi-fi insegura. [Em linha]. Disponível em: <https://www.kaspersky.com.br/blog/como-evitar-uma-rede-wi-fi-insegura/3593/>. Acesso em: 22 jan. 2018.

Segundo o parágrafo anterior, apenas uma simples conexão em uma rede wireless que até então seria inofensiva, gerou várias violações fundamentais de direitos e garantias na vida deste usuário, como a violação da vida privada, de correspondência por exemplo, e futuramente caso os equipamentos com chip e internet forem hackeados[13], caberá com certeza alguns dos delitos expressos no tópico 3 desta escrita.

Em consequência desta falta de segurança em redes wireless, se recomenda que os usuários nunca se conectem em redes que tenha certeza desta segurança como em sua casa e ou trabalho (caso o trabalho possua medidas de segurança). E ainda assim não fornecer a sua senha de internet residencial para exclusivamente ninguém.

Seguem algumas medidas expressas pela Microsoft (2017)[14] para que se obtenha uma maior segurança acerca de violação de dispositivos informáticos:

- Não visitar sites não seguros, suspeitos ou falsos;
- Não abrir emails e anexos de email que você não estava esperando ou enviados por pessoas que você não conhece. (situação abordada nesta escrita);
- Não abrir links mal-intencionados ou ruins em emails, Facebook, Twitter e outras postagens de mídias sociais ou em chats de mensagens instantâneas, como o Skype.
- Manter seu computador atualizado com a versão mais recente do sistema operacional;
- Fazer backup do conteúdo em seu computador com regularidade;
- Manter duas cópias de segurança dos dados do computador, em dispositivos distintos.

Outros autores, como o Cleórbete Santos[15], profissional de Segurança da Informação, seguem algumas das suas medidas:

- Buscar utilizar o melhor antivírus e o navegador mais seguro;
- Manter atualizados o Windows, aplicações instaladas e antivírus;
- Nunca abrir anexos sem ter certeza da origem;
- Usar firewall;
- Nunca usar softwares não originais.
- Proteção das Informações por Backup (como política de segurança).

Assim como a Kaspersky (2017)[16] que é uma das grandes empresas mundiais quando se fala em segurança da informação, fala que:

- Devem ser evitadas redes sem fios desconhecidas.

13 Hackeados: violação de segurança por hacker / cracker.

14 MICROSOFT. Proteger seu computador contra ransomware. 2017. [Em linha]. Disponível em: <https://support.microsoft.com/pt-br/help/4013550/windows-protect-your-pc-from-ransomware>. Acesso em: 15 dez. 2017.

15 SANTOS, Cleórbete. Muito Além do Antivírus. Palmas: [s.e.], 2017. [Edição do Kindle].

16 Kaspersky. Milhões de Smartphones Vulneráveis a Pontos Falsos. [Em linha]. Disponível em: <https://www.kaspersky.com.br/blog/milhoes-de-smartphones-vulneraveis-%E2%80%8B%E2%80%8Ba-pontos-falsos-de-wi-fi/3535/>. Acesso em: 22 jan. 2018.

Diante do crescimento da conduta de oferecer acesso a internet grátis através de redes sem fio, por estabelecimentos, cria-se uma brecha para que pontos de acesso falsos sejam criados por hackers mal-intencionados com finalidades ilícitas diante dos dispositivos que conectarem nesta. Mas caso o usuário necessite o acessar a internet por uma rede pública seguem algumas das medidas propostas pela Kaspersky (2017)[17]:

- Desconfie de todos os pontos de acesso;
- Tente verificar a legitimidade do ponto de acesso;
- Use uma VPN (Virtual Private Network);
- Evite acessar sites específicos (redes sociais ou bancos, por exemplo);
- Proteja seu dispositivo.

As medidas de segurança são básicas e simples, e ainda assim é a principal ferramenta de proteção que um usuário pode proporcionar para si mesmo. Todo esse procedimento de segurança é de extrema necessidade para se manter tantos os dispositivos pessoais seguros, seja computador, smartphone ou equipamentos IoT.

3 CONSIDERAÇÕES FINAIS

Tecnologicamente, estamos sempre no modo evolução ativo, diante de uma sociedade que cada vez mais necessita da tecnologia para facilitar a vida de nós, seres humanos, através das inovações que fazem com que a informação seja cada vez mais automática.

Estamos vivendo em uma cibercultura onde cada vez mais termos facilidades acessíveis através dos dados que produzimos, sejam direcionados a outros humanos, sejam coletados pelas máquinas. E quando se fala em máquina que pode compreender, surge o viés da IoT (*Internet of Things*), Internet das Coisas, que através de um chip de processamento buscarão cada vez mais entender as nossas necessidades, agilizando os resultados que pretendemos.

As coisas com internet, ou seja, as máquinas cada vez terão mais acesso a nossas privacidades e intimidades, e expostas a tanta informação que sequer realizamos produzir, acabarão por perceber eventos e pessoas sem mesmo que percebamos. Mas ao saber tanto sobre nós mesmos, juntamente com nossa acomodação em ter tantos serviços com esforço mínimo, estamos sob o risco das consequências dessa união, visto que o fato de um equipamento IoT hackeado dar acesso a dados completos da vida privada e a intimidade de alguém, para outrem, de má-fé.

Algumas medidas básicas poderão ser buscadas para minimizar tais riscos, e ainda que os equipamentos possuam meios de segurança nativos, como também a responsabilidade dos governos em prover segurança seja vital, os usuários será a principal ferramenta de proteção diante de suas atitudes, passando assim a ter papel fundamental nesse cenário de fluxo incontável de informação.

17 Kaspersky – Segurança em Redes Wi-Fi Públicas. [Em linha]. Disponível em:<https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi>. Acesso em: 22 jan. 2018.

REFERÊNCIAS

BRASIL. CÓDIGO Penal Brasileiro - **Decreto-Lei 2.848/1940, de 07 De dezembro**. [Em linha] Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html>. Acesso em: 20 set. 2017.

COELHO, Pedro. **Internet das Coisas**: Introdução Prática. Lisboa: FCA. 2017.

KASPERSKY: **Como Evitar uma rede wi-fi insegura**. [Em linha].Disponível em: <https://www.kaspersky.com.br/blog/como-evitar-uma-rede-wi-fi-insegura/3593/>. Acesso em: 22 jan. 2018.

_____ **Milhões de Smartphones Vulneráveis a Pontos Falsos**. [Em linha]. Disponível em: <https://www.kaspersky.com.br/blog/milhoes-de-smartphones-vulneraveis-%E2%80%8B%E2%80%8Ba-pontos-falsos-de-wi-fi/3535/>. Acesso em: 22 jan. 2018.

_____ **Segurança em Redes Wi-Fi Públicas**. [Em linha].Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi>. Acesso em: 22 jan. 2018.

MELLO, Celso Antônico Bandeira de. **Curso de Direito Administrativo**. 32. ed. São Paulo: Malheiros. 2014.

MICROSOFT. **Proteger seu computador contra ransomware**. 2017. [Em linha]. Disponível em: <https://support.microsoft.com/pt-br/help/4013550/windows-protect-your-pc-from-ransomware>. Acesso em: 15 dez. 2017.

SANTOS, Cleórbete. **Muito Além do Antivírus**. Palmas: [s.e.], 2017. [Edição do Kindle].

UNDERSINGER, Martin. **Anonymay sur Internet**. Paris: Eyrolles. 2016.