A PROTEÇÃO DE DADOS DENTRO DAS FÁBRICAS INTELIGENTES CRIADAS PELA INDÚSTRIA 4.0

Dienifer Ferreira da costa[1]
GuilhemeWunsch[2]

RESUMO:

As transformações causadas pela Indústria 4.0 têm gerado uma grande reviravolta em todos os seguimentos, seja na vida do trabalhador, fazendo com que este tenha que lidar com a sua iminente substituição dos postos de trabalho em virtude da automação, bem como com o potencial vazamento de seus dados pessoais armazenados na rede. Assim, para sobreviver a esta revolução industrial e usufruir ao máximo dos benefícios proporcionados por esta nova fase, as fábricas terão que ser cada vez mais flexíveis, a fim de se adequar aos novos cenários apresentados pelas constantes transformações tecnológicas. As tecnologias criadas pela Indústria 4.0, têm sido objeto de muito debate no mundo todo, visto a necessidade de se analisar de que forma se dará a segurança cibernética quanto as questões de transferência e o armazenamento de dados dentro das fábricas inteligentes, que envolvem desde a cadeia produtiva à gestão do negócio, fazem com que a confiabilidade e a segurança dos bancos de dados sejam colocadas à prova.

PALAVRAS-CHAVE: Proteção de dados. Indústria 4.0. Tecnologias.

INTRODUÇÃO

[1]Graduada em Direito pela Universidade do Vale do Rio dos Sinos – UNISINOS. Assessora jurídica. Integrante do grupo de Pesquisa Cibertransparência, do Programa de Pós-Graduação em Direito (PPGD) da Unisinos.

[2] Pós-Doutor em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Doutor em Direito pela Universidade do Vale do Rio dos Sinos - UNISINOS. Mestre em Direito pela Universidade do Vale do Rio dos Sinos - UNISINOS. Professor Permanente do Mestrado Profissional em Direito da Empresa e dos Negócios da Universidade do Vale do Rio dos Sinos - UNISINOS. Professor do Curso de Direito da Universidade do Vale do Rio dos Sinos - UNISINOS, em São Leopoldo,RS. Professor e Advogado do PRASJUR - Prática de Assistência Judiciária Gratuita, da Universidade do Vale do Rio dos Sinos - UNISINOS. Coordenador do Curso de Pós-Graduação em Direito do Trabalho e Processo do Trabalho da Universidade do Vale do Rio dos Sinos - UNISINOS. Membro do grupo de pesquisa Direito do Trabalho e Novas Tecnologias, liderado pela Professora Drª. Denise Pires Fincato (PUCRS). Coordenador da Comissão Especial de Direito do Trabalho da OAB/RS - Subseção São Leopoldo. Autor de livros e artigos. Acadêmico Titular da Cadeira número 26 da Academia Sul-Rio-Grandense de Direito do Trabalho. Advogado.

Com o advento da Indústria 4.0, a humanidade precisou percorrer um longo caminho marcado por três revoluções industriais, cujas particularidades e objetivos estavam voltados a tirar o homem do campo, para colocá-lo nos centros de produção manufatureira onde surgiam as primeiras máquinas industriais.

Contudo, na busca por novas tecnologias capazes de proporcionar uma cadeia produtiva cada vez mais rápida, inteligente, eficiente e autônoma; estas inovações tecnológicas acabaram ocasionaram o surgimento da Quarta Revolução Industrial, a famosa Indústria 4.0.

Com o implemento deste novo modelo industrial, diversos impactos passaram a refletir em aspectos importantes dentro da empresa, como: a dinamização dos meios de produção, e sobretudo no modo de se controlar os processos de produção, armazenamento de dados, informações tudo através das tecnologias que cabem na palma da mão. Isto porque, as tecnologias desenvolvidas pela Indústria 4.0 estão relacionadas aos sistemas mais dinâmicos e interconectados.

Assim, a questão do direito a proteção de dados pessoais na era de maior desenvolvimento de tecnologias informacionais nunca esteve tão enfoque e ao mesmo tempo desprezado por muitas empresas, inclusive brasileiras.

Visto que por haver uma infinidade de unidades produtivas interconectadas, a segurança de dados e informações passa a ser uma das preocupações enfrentadas pelo profissional moderno, pois a ausência de mecanismos capazes de elidir invasões e espionagem industrial, faz com que se tornem brechas suficientes para que ocorram os ataques cibernéticos por vírus e *hackers*, fazendo com que sejam implementados meios de proteção de dados focados às empresas que se adaptaram a Indústria 4.0, tornando-se assim as chamadas fábricas inteligentes.

1 O papel da segurança de dados na modelagem da Indústria 4.0

Com o surgimento de uma nova era industrial que coloca as empresas em um novo patamar nos quesitos de produtividade, eficiência e gestão, ao promover a automação dos processos de fabricação e o armazenamento de dados na nuvem, demonstram que o chão da fábrica está mudando, ao conectar os componentes físicos aos sistemas cibernéticos, fazendo com que essa interação seja a engrenagem que promete sustentar a indústria do futuro(PIRAMIDAL, 2018).

É sabido que a Indústria 4.0 está completamente associada às tecnologias e como estas atuam nos processos de produção. Porém, o que muito se ignora, é o fato de que estas mesmas tecnologias também estão relacionadas ao grande volume de coleta e análise de dados.

Uma das inovações da indústria do futuro que tem feito brilhar os olhos dos revolucionários industriais é a possibilidade de conexão e geração de dados entre as máquinas, equipamentos e *softwares* de gerenciamento (A VOZ DA INDÚSTRIA, 2018).

Essa possibilidade permitirá o controle todo o processo industrial, desde a separação dos insumos até o produto final, detectar falhas e corrigi-las imediatamente, bem como gerenciar as financeiras através de um *smartphone,* representam alguns dos pontos que elevam ao máximo o nível de desenvolvimento de uma empresa.

Contudo, esse gerenciamento moderno só será possível através da captura de grande quantidade de dados, que por meio de *softwares* permitirão que essas inovações realmente se efetivem. Porém, por se tratar de uma revolução com as mudanças mais significativas já presenciada pela humanidade, os efeitos da Quarta Revolução ultrapassam as fronteiras das inovações tecnológicas e do mercado de trabalho. Isto pois, com a circulação frenética de dados em uma rede de computadores que possui dimensão infinita, surge mais uma preocupação: a segurança e a proteção dos bancos de dados das empresas modernas.

Por conta disso, a cibersegurança ainda tem sido um dos obstáculos na implementação de muitas tecnologias criadas na indústria moderna, pelo fato dos sistemas industriais serem a essênciadentro da fábrica, e se ocorrer um ataque cibernético, será o ponto de maior impacto(ALMEIDA, 2018).

Para o analista de segurança da informação, Rafael Taissun(2018): “sensores fabris de temperatura, pressão, densidade, velocidade de esteira, entre outros exemplos

estão interligados e se comunicando com uma central, responsável por analisar e coletar dados gerados a cada segundo". Logo, percebe-se que é feito uma coleta incalculável de dados relacionados a todos os processos e atividades desenvolvidas dentro de uma empresa e que requerem proteção.

A insegurança que paira na mente dos empreendedores da indústria moderna é legítima, pois ao entrar no campo de dados e sistemas digitais, a segurança do negócio passa a estar ameaçada, isto porque além do roubo de informações, será preciso lidar com outras espécies de crimes cibernéticos, sendo que muitas empresas já foram vítimas desses crimes, em virtude de sua vulnerabilidade na rede mundial de computadores, podendo inclusive paralisar toda uma cadeia produtiva provocada por esses ataques.

Para tanto, a Federação das Indústrias do Estado de São Paulo (FIESP), realizou uma pesquisa a fim de averiguar em questão de números, quantas indústrias brasileiras já foram vítimas de ataques cibernéticos. O estudo mostrou que apesar de 92% das empresas entrevistas terem consciência da importância de se investir em segurança de dados, 31% delas já sofreram algum tipo de ataque digital, sendo que a percentagem de indústrias que afirmam possuir uma infraestrutura adequada para suportar as inovações da Quarta Revolução compreende apenas 18%(ALMEIDA, 2018).

O resultado dessa pesquisa mostra o quanto esse assunto não é uma das prioridades para as fábricas internas, sendo que ironicamente, essas empresas encontram-se despreparadas e para o futuro tecnológico que as aguarda.

Quanto a essa temática, é importante salientar que antes mesmo da reconfiguração produtiva, as indústrias já estavam expostas aos altos riscos de segurança operacional, contudo, essas ameaças encontravam apenas no espaço físico. Hoje, com a apresentação da Indústria 4.0, não apenas o ambiente fabril está a mercê de ameaças, pois agora elas podem ocorrer sem que o criminoso saia de casa, pois tudo se dá no ciberespaço (NETEYE, 2018).

Outrossim, esse tipo de risco tende a ganhar mais relevância no decorrer dos anos, pois só no Brasil já temos milhares de caso de vazamentos de dados, sendo um dos mais lembrados, o caso de divulgação de mais de 350 credenciais de acesso de usuários de sites de *e-commerce*, como a *Netshoes,* Magazine Luiza, Ponto Frio, Extra, Casas Bahia, Centauro, PagSeguro entre outras; além de que em alguns casos ainda houve o exposição de números de cartões de crédito e dígitos de segurança (COSTA, 2017).

Para o Diretor de segurança cibernética, Leonardo Lemes, os perigos cibernéticos surgiram desde a Terceira Revolução Industrial, porém, que foram agravados na atual Revolução, por possuir uma superfície de ataques mais amplos. O autor ainda relaciona algumas das características que mais contribuem para a insegurança na questão de proteção de dados, quais sejam: "interface homem – máquina, engenharia social, códigos maliciosos, senhas fracas, ataques baseados na *web*, falhas de configuração, monitoramento e roubo de dados, acesso físico, ataques aos sistemas de comunicação, comunicação entre máquinas" (NETEYE, 2018).

Apesar de serem exemplificados apenas alguns meios, percebe-se que para questões de segurança de dados isso representa ser algo significativo, pois para *hackers* e pessoas mal-intencionadas esses meios consistem em brechas para invadir sistemas e coletar dados até então sigilosos.

Neste sentido, a Pesquisa Anual de Riscos Globais de Segurança de Tecnologia da Informação de 2017, constatou-se que das 962 empresas pesquisadas, 28% delas sofreram ataques e ameaças nos últimos 12 meses. Essa percentagem representa 8 pontos percentuais a mais do que o ano de 2016 (SANTI, 2018).

Os dados apresentados na pesquisa revelam o quanto o tema da segurança no ciberespaço merece atenção redobrada. Sobre esse aspecto, o gerente de Produtos de divisão *Industrial Automation* da ABB Brasil, Marcos Hillal se posiciona dizendo que passou-se a ter uma preocupação maior quanto aos ataques cibernéticos no momento da migração da automação para o campo de TI, mas que no entanto, as empresas não devem ver isso como uma barreira ao fazerem uso das tecnologias, que irão proporcionar para o negócio o alcance da otimização e redução de custos.

Neste ínterim, Eduardo Almeida(2018) assim também pontua:

> O crescimento do uso de tecnologia nos sistemas industriais, principalmente focado na combinação entre IoT (Internet ofThings) e Inteligência Artificial, tem otimizado os processos fabris, aumentando a produtividade e diminuindo falhas de fabricação. Porém, o avanço da conectividade também traz preocupações sobre o sigilo dos dados compartilhados na rede.

No entanto, a segurança de dados não é uma das prioridades nos processos de automação fabril dentro do território brasileiro, pois o elevado número de empresas que já sofreram ataques cibernéticos demonstra isso.

Contudo, Rafael Taissun(2018) alerta que os dados mesmo não sendo sigilosos, se caírem em mãos erradas, pode haver grande prejuízo para a empresa, como o acesso

a projetos de novos produtos, acesso às fórmulas químicas de um produto ou a senha utilizada na portaria eletrônica, exemplifica o analista (ALMEIDA, 2018).

Ainda para o especialista, os riscos à segurança de dados estão ligados às questões de disponibilidade, confidencialidade e integridade, pois na sua percepção:

> como exemplo temos os dados de clientes que são vazados ao público em geral (confidencialidade), sistemas que deixam de operar devido a falhas técnicas (disponibilidade) e alterações de informações em bancos de dados que causam o processamento errado de dados (integridade) (A VOZ DA INDÚSTRIA, 2018).

Isso porque, esses três atributos correspondem na garantia da segurança da informação. Neste sentido, importante se faz conceituar cada um deles.

A confidencialidade consiste na "imposição de limites de acesso à informação apenas às pessoas e/ou entidades autorizados por aqueles que detêm os direitos da informação. Ou seja, somente pessoas confiáveis podem acessar, processar e modificar os dados" (LUCENA, 2017).

Por sua vez, a integridade refere a conservação de todas as características originais das informações em questão, estando ligados a manutenção e destruição dos dados. Já a disponibilidade é a garantia de que os dados sempre estarão disponíveis para o uso, desde que forma legítima(LUCENA, 2017).

O consenso dos especialistas é unânime neste cenário, no mínimo, assustador, ao concordarem que não basta que as empresas investirem em pessoal, processos e tecnologia como forma de proteção, frente aos riscos cibernéticos, pois na visão de Flávio de Sá, gerente de linhas financeiras da AIG do Brasil, "o Brasil sempre esteve entre os países mais atacados. Antes amarelo, agora o farol ficou vermelho para as empresas" (MARTINS, 2018).

Para Maurício Bandeira, ainda faltam conhecimento das empresas sobre os reais prejuízos que um ataque virtual pode causar nos negócios, pois para ele o risco cibernético percorre toda a cadeia produtiva, e uma invasão pode provocar consequências catastróficas, que podem ir desde uma paralisação da produção até reparações de danos milionárias.

Porém, um dos grandes problemas que envolvem a segurança de TI parte do fato de que o próprio indivíduo abre mão dessa proteção, como observa o filósofo político Michael Sandel (2015): "parece que estamos cada vez mais dispostos, por conveniência, a negociar nossa privacidade com muitos dispositivos que usamos rotineiramente".

Apesar de grande parte dos setores administrativos das empresas já estarem há um longo tempo utilizando as plataformas digitais, como a nuvem para armazenar e transferir dados em tempo real, que podem ser acessados em qualquer dispositivo e em qualquer tempo, não quer dizer que não haverá inseguranças quanto ao sigilo desses dados, pois para o chão da fábrica esse conceito de automação ainda é um tema novo e desconhecido.

A confiabilidade na segurança da informação é algo imprescindível dentro da fábrica inteligente, isto pois, antes o ambiente digital era mais familiar em setores como RH, Marketing e TI, porém, não para a área da operação (GONÇALVES, 2018).

Na visão do diretor de segurança cibernética da Kroll no Brasil, Marcelo Matinez (2018), "O nível de maturidade de segurança da informação nas empresas ainda é muito baixo. Tanto é que às vezes não existe uma equipe responsável por essa área", pois para ele: "a segurança cibernética vai além da proteção dos ativos tecnológicos, por exemplo, computadores, *softwares* e *hardwares*. Envolve, ainda, processos e conscientização dos profissionais. "Entre esses pilares de proteção, o elo mais fraco é a falta de conscientização das pessoas" (MARTINS, 2018).

Assim, por estar lidando com uma enorme circulação de dados, irá requerer da indústria digital, uma infraestrutura ainda mais eficiente para suportar os efeitos que a Indústria 4.0 trará, para que não haja uma vulnerabilidade das informações sigilosas daquele negócio, pois o problema da segurança de TI não consiste apenas no roubo das informações, mas também no abalo da cadeia produtiva em decorrentes dos ataques e invasões cibernéticas, que não se limitaram a um único dispositivo, mas tornará vulnerável e passível de exploração toda a cadeia de produção (TELIUM, 2017).

Ainda nessa temática, *mister* se faz relatar que, conforme explanado por Ricardo Gonçalves (2018), a questão das invasões e coleta ilegal de dados, não são apenas praticadas por *hacker*, pelo contrário, ao ser analisado o longo histórico das incursões cometidas, fica evidente que na maioria dos casos, foram os próprios funcionários que vazaram as informações da empresa para quem prestam seus serviços.

Em termos de pesquisa, segundo o estudo realizado pela GARTNER divulgada em 2015, o percentual de 95% das falhas compreendendo *cloudcomputing*tem como responsáveis os próprios usuários (GONÇALVES, 2018), tirando a culpa das costas da tecnologia.

Para fins exemplificativos, relembra-se do caso *Wikileaks*, que se refere ao vazamento de dados da CIA, que acabou exposto um volume de dados considerados

confidenciais dos Estados Unidos. Neste episódio de invasão aos dados sigilosos de um dos países mais potentes do mundo, acreditava-se que o responsável por todo esse crime cibernético seria um *hacker*, porém, para a surpresa de todos, foi um ex-funcionário que facilitou o acesso dos dados à terceiros (GONÇALVES, 2018).

Todavia, é preciso atentar para o fato de que nem sempre o vazamento de dados se dará de forma dolosa, pois um dos principais motivos de vazamento de informações da nuvem por meio de funcionários é o decorrente do total despreparo e falta de treinamento dos colaboradores para enfrentar esses nossos desafios que a Indústria moderna vem instaurando.

Outrossim, embora para alguns as novidades ocasionadas pela implementação desta Revolução contemporânea gere insegurança, para Ricardo Gonçalves (2018) a sua visão é mais positiva:

> Quando olhamos para a indústria é fácil perceber a rapidez com que ela vem evoluindo. A chamada Internet Industrial tem um papel importantíssimo para o crescimento do País, principalmente ao que se refere às inovações tecnológicas efetivas e seguras. Os robôs adotados nas fábricas passam por constantes manutenções preventivas para garantir que não haja nenhum erro que os tornem vulneráveis, pelo contrário, eles são preparados para desenvolverem suas atividades em sintonia com as demais máquinas e pessoas, contribuindo - e muito! - para o desenvolvimento da nova economia.

Contudo, na medida que as tecnologias forem evoluindo, as infraestruturas de TI devem igualmente seguir o mesmo fluxo de desenvolvimento, tendo em vista as informações serem incontroláveis na rede e se expostas, podem causar grandes danos para os negócios, ao invés de proporcionar os benefícios que a Indústria 4.0 veio oferecer.

As tecnologias que surgem a cada dia são criadas com o objetivo de transformar e otimizar todos os processos produtivos, no entanto, o segurança desses dados deve ser uma prioridade dentro das fábricas inteligentes (ALMEIDA, 2018).

A seguridade de dados dentro da Revolução contemporânea terá papel fundamental na proteção das informações contra cibercrimes, alteração de dados e espionagem industrial. Mas para que a segurança de TI se efetive dentro das fábricas inteligentes, será preciso instaurar políticas de segurança, controles de acesso que será melhor explanado em tópico próprio.

2 A atuação do direito à proteção de dados no ambiente industrial digital

As movimentações tecnológicas ocorridas no decorrer dos anos, fez com que a transferência e o armazenamento de informações ocorressem em uma magnitude e velocidade cada vez maior. Diante deste contexto, a autora Laura Mendes(2014, p. 37) menciona que, na busca por tutelar a personalidade do indivíduo, contra os possíveis riscos no âmbito do tratamento de dados pessoais, é que a proteção de dados pessoais passou a desempenhar um papel fundamental no cenário tecnológico, o qual se encontram dentro e fora da fábrica.

Um aspecto importante de ser ressaltado a respeito da proteção de dados, é que a sua função não consiste em proteger os dados pessoais propriamente, mas sim, proteger a pessoa titular desses dados. Isto porque, na visão de Danilo Doneda (2006, p. 27), ao se considerar a velocidade em que ocorrem as trocadas e os tratamentos das informações, aumenta-se a probabilidade de haver vazamentos de dados, que poderão causar graves violações à personalidade da pessoa ao ter seus dados divulgados perante outrem (DONEDA, 2006, p. 27).

Para a autora Laura Schertel Mendes (2014, p. 37), a disciplina da proteção de dados sempre esteve em substancial mudança, em virtude das transformações nos âmbitos econômicos, sociais e tecnológicos ocorridos nas últimas quatro décadas, para que se possam compreender "os desafios constantes que a tutela jurídica dos dados pessoais enfrenta, assim como para a análise das perspectivas da proteção de dados no futuro".

Neste ínterim, ao considerar as transformações que se encontram em curso devido às implementações das Tecnologias da Informação criadas na Indústria 4.0, que acabam abrangendo não apenas as fábricas em si, mas também, todo e qualquer segmento que envolva as inovações digitais, fazem com que se tenha uma maior preocupação quanto aos direitos de proteção de dados no ambiente virtual, frente aos milhares de ataques ocorridos no ciberespaço (MENDES, 2017, p. 37).

Isto porque, na sociedade da Indústria 4.0, todos os dias são deixados "rastros" nas mais diversas atividades cotidianas, as quais podem consistir desde o fornecimento do número do CPF em uma compra realizada em um *site,* o registro biométrico no banco para realizar transações, até mesmo dar "*likes"* em publicações do *Facebook,* são classificados como rastros, pois através desses atos gera-se uma análise preditiva das

preferências do usuário sobre determinados temas curtidos na rede social, o que nada mais é do que uma coleta e análise de dados pessoais.

Tendo em vista a Indústria 4.0 ser o novo paradigma informacional, necessário se faz reproduzir o seguinte trecho do Livro "Privacidade, proteção de dados e defesa do consumidor", uma vez que aborda esta temática de forma concisa e esclarecedora:

> Nesse sentido, é fundamental que o debate sobre a proteção de dados pessoais tenha como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade, rejeitando-se a ideia de que ela é a responsável pela per- da de privacidade pessoal da sociedade contemporânea. Isto é, não é a tecnologia em si a causa do problema da privacidade, mas as decisões que tomamos em relação à tecnologia. Sob essa ótica e para possibilitar a resposta adequada aos desafios sociais advindos da revolução tecnológica, é fundamental que a teoria do direito se reconstrua a ponto de compreender e solucionar os novos problemas enfrentados pelo homem na era da informação. (...) Nesse contexto de desenvolvimento da tecnologia de informação, o direito à privacidade transforma-se para dar origem à disciplina da proteção de dados pessoais, de modo a se adaptar aos de- safios impostos pelo avanço da técnica. Assim, a proteção de dados pessoais pode ser compreendida como uma dimensão do direito à privacidade, que, por consequência, partilha dos mesmos funda- mentos: a tutela da personalidade e da dignidade do indivíduo (MENDES, 2014, p. 35).

Sob essa ótica, antes mesmo do surgimento da Quarta Revolução, já havia a necessidade da tutela jurídica para proteger os dados dos cidadãos, em razão de que as informações pessoais possuem conteúdo econômico e passível de comercialização, conforme salienta a Doutora Têmis Limberger (2007, p. 58) integrante da Rede Ibero-americana de proteção de dados:

> As novas tecnologias tornam a informação uma riqueza fundamental da sociedade. Os programas interativos criam uma nova mercadoria. O sujeito fornece os dados de uma maneira súbita e espontânea e, por conseguinte, depois que estes são armazenados, esquece-se de que os relatou. Por isso, é um desafio oferecer proteção à intimidade com relação a esses serviços.

Porém, a legislação que visa proteger os direitos de dados pessoais por muito tempo foi escassa, sendo que durante muitos anos o maior dispositivo legal sobre essa temática era a Directiva Comunitária 95/46 da União Europeia, que colaborava com a solução de casos envolvendo problemas de vazamento e violação de dados em países comunitários.

Por ser um regulamento considerado ultrapassado, tendo em vista os incontáveis avanços da tecnologia e surgimento de nossos problemas neste cenário, necessário

também se fez, a atualização das ciências jurídicas para resguardar direitos eventualmente violados.

Assim, em 25 maio de 2018, entrou em vigor a Resolução 2016/679 da União Europeia, comumente conhecida como GDPR (*Geral Data ProtectionRegulation*), a qual é uma "modernização" da DC 95/46 CE, cujo objetivo é a proteção dos dados pessoais, trazendo conceitos e inúmeras regras, voltadas aos responsáveis por tratamento e processamento de dados, cujos efeitos atingirão inclusive, empresas brasileiras (MOREIRA, 2017).

A GDPR veio para aplicar uma rígida disciplina em todas as empresas e organizações, independentemente do porte ou ramo de atuação, no que se tratar de coleta, processamento, compartilhamento de dados. Permitir que o usuário decida como os seus dados serão processados e se serão processados, saber quais dados e para qual finalidades estes serão analisados, são algumas das obrigações que recaem sobre as entidades que realizarem esse serviço de coleta e estudos dos dados, sendo ainda, em determinadas situações, as empresas terão que ter a sua disposição, um executivo que supervisionará o tratamento desses informações e esclarecer o ocorrido à sua autoridade (ALECRIM, 2018).

Apesar de ter prevalência na União Europeia, a Regulamento Geral de Proteção de Dados – GDPR tem a incidência de seus efeitos também no território brasileiro, pois se, por exemplo, uma loja *online* brasileiro ou de qualquer outro país que quiser exportar produtos para clientes que se encontram em solo da União Europeia, terá que obrigatoriamente se adequar as regras estipuladas pela GDPR sob pena de desrespeitar a lei (ALECRIM, 2018).

Isso justifica o envio de milhares de e-mails informando sobre as novas políticas de privacidade quando o regulamento estava para entrar em vigor, justamente para avisar sobre o rigoroso sistema que estava sendo implantado, cujo raio de alcance seria mundial.

Em virtude desse disparo de correspondências eletrônicas, as companhias começaram a adaptar seus sistemas, a fim de evitar qualquer violação ao regulamento, pois em caso de descumprimento, as multas podem consistir em desde o recebimento de uma simples notificação em caso de infração leve, até a aplicação de uma multa de € 20 milhões ou de até 4% sobre a receita anual global da companhia, o que for maior. Isso significa que, no caso de companhias como *Google, Microsoft* e *Facebook*, a punição pode custar bilhões de dólares, na visão de Emerson Alecrim(2018).

Todavia, no Brasil a GDPR representa algo mais, pois foi seguindo o seu modelo, foi aprovado a Lei Geral de Proteção de Dados Pessoais brasileira nº 13.709, de 14 de agosto de 2018 – LGPD, a qual dispõe sobre: uso, armazenamento, tratamento de dados, objetivando em especial, a garantia e o controle de dados pessoais dos indivíduos, de uma forma que as referidas práticas se deem se forma mais transparente e segura. Se buscou criar um modelo normativo que fosse moderno para proporcionar um grau de proteção que se encontre no padrão internacional (BENTO, 2018).

Através desta legislação interna de proteção de dados, haverá uma maior efetivação na tutela jurídica e, consequentemente, punições mais rígidas diante de descumprimentos. Para tanto, o especialista de Políticas e Indústria da CNI, Fabiano Barreto (2019), assim define a LGPD:

> A Lei Geral de Proteção de Dados (LGPD) é a norma que estabelece direitos e obrigações específicos, para usuários e empresas, sobre tratamento de dados pessoais. Até então, existiam apenas normas gerais de proteção à privacidade. A criação da LGPD era uma demanda por atualização legislativa a fim de acompanhar a transformação digital, com enormes volumes e fluxos de informações pessoais.

Apesar de entrar em vigência apenas em 15 de fevereiro de 2020, as empresas possuem 18 meses para se adequarem as novas regras, o que não será um problema para as empresas que atuam no mercado internacional, em virtude de já estarem familiarizadas com a GDPR, conforme pontua Beatrice Bento(2018).

Assim, como está no regulamento da UE, a nova lei brasileira institui normas claras e preventivas sobre qualquer tipo de uso de dados, que deverá se submeter aos princípios da finalidade e necessidade, ou seja, a LGPD visa limitar o acesso aos dados de terceiros apenas para casos específicos, devendo tomar como medida, o aviso ao titular dos dados que seus dados estarão sendo analisados.

Neste sentido, no entender da autora Beatrice(2018)

> Os dados pessoais são definidos como informações relacionadas a pessoa natural identificada ou identificável. Além disso, a LGPD, de maneira análoga ao GDPR, traz a definição e cria regras específicas para o tratamento de dados sensíveis (relativos à origem racial, étnica, opiniões políticas, vida sexual e outros), que somente pode ser realizado mediante o consentimento do titular, de forma específica e destacada, para finalidades específicas, assim como define regras específicas para o tratamento de dados de crianças e adolescentes, que dependerá do consentimento dos pais ou responsáveis.
> No entanto, há circunstâncias em que o consentimento do titular dos dados pode ser dispensado, como: a utilização de dados para cumprimento de obrigações legais, o cumprimento de execução de políticas públicas, a proteção da vida do titular ou de terceiros, entre outros.

Todo esse cuidado e dever de informação aos titulares dos dados, possuem justamente o alvo de por em prática, ou pelo menos tentar prevenir o acesso não autorizados de dados coletados, além de cientificar casos de coletas ilícitas, acidentais ou destruição dos mesmos, a fim de evitar ao extremo que novos ataques cibernéticos venham acontecer (BENTO, 2018).

Sob esse prisma de salvaguarda de direitos, é relevante analisar a situação das empresas, ou seja, pessoas jurídicas também detentoras de direitos, quanto a proteção de dados pessoais. Antes de mais nada, necessário se faz definir o conceito de dados pessoais. Para tanto, o mesmo é definido no próprio regulamento em seu art. 5º, o qual diz que dado pessoal é: "informação que relacionada a pessoa natural identificada ou identificável" (BRASIL, 2019).

Neste sentido, pode-se compreender que dado pessoal são as informações que instantaneamente já se pode identificar o seu titular, através do nome, número do CPF e demais informações pessoais. Assim, se ocorrer qualquer tipo de coleta de dados dentro da fronteira brasileira, realizado por pessoa física ou jurídica, de direito público ou privado, que tenha como finalidade oferecer produtos ou serviços no Brasil, estará coberto pelo manto da LGPD.

Porém, o que importa neste momento é o termo "pessoa natural". Mediante se verifica no próprio texto legal, o direito a proteção de dados abrange apenas as pessoas naturais, consequentemente, deixando de incidir a Lei Geral sobre os dados de pessoas jurídicas. Assim, para que haja aplicação de proteção de dados da pessoa jurídica, terá que haver a prática de condutas ilegítimas que coletem dados pessoais dos sócios, diretores e funcionários, pois neste caso, são pessoas físicas (VENTURA, 2018).

Contudo, dentro de uma fábrica não são apenas os dados de sócios e funcionários que podem ser violados, há uma gama de informações que se encontra a mercê dos maus intencionados que estão à procura de vítimas os seus cibercrimes, o que infelizmente, não é algo incomum, conforme já mencionado anteriormente.

Toda a coleta e análise de dados sigilosos de empresas, relacionadas às informações como: criações de novos produtos ainda não anunciados ao mercado, fórmulas das invenções, informações de funcionários e de faturamento, cadeia de produção entre muitas outras; geram série de preocupações, visto que os prejuízos decorrentes de espionagem industrial, roubo de informações ou adulteração de dados salvos na nuvem, podem danos avaliados em milhões de reais.

Conforme constata-se acima, com o advento da LGPD, as empresas terão que se adequar às novas regras que se instauram quanto à proteção de dados pessoais de terceiros, porém, em não atendendo as especificações não poderão escapar das pesadas penalidades que cairão sobre os seus ombros.

Todavia, neste ínterim, é intrigante o fato de que para as essas mesmas empresas não há qualquer previsão de proteção de seus dados, pois ao ponto de que as fábricas analisam dados de outros, essas também possuem dados passíveis de análises. Assim, a pergunta que paira é: como as empresas poderão proteger seus dados frente à inércia do legislador em estipular leis de proteção para um setor que é amplamente atingido pelos efeitos das tecnologias consequentes da Indústria 4.0?

Como não ainda não há qualquer previsão para aprovação de leis sobre essa temática, e sempre com a senso de apreensão quanto à ocorrência de ataques cibernéticos, o que resta para as empresas é a adoção de medidas de segurança que serão melhor explicitadas no tópico a seguir.

3 Os desafios da segurança de TI e os mecanismos de controle e proteção de dados para a infraestrutura da Quarta Revolução Industrial

A Indústria 4.0 representa o ápice das inovações tecnológicas que transcendem o campo industrial para estar inserido na vida da sociedade em geral. Porém, neste novo modelo de reestruturação, uma das tecnologias considerada como um dos pilares da Quarta Revolução é - o armazenamento e compartilhamento de uma infinidade de dados em tempo real.

Esse infinito emaranhado de dados armazenados na rede mundial de computadores pode ser gerado tanto por pessoas físicas quanto jurídicas, e que trazem consigo grande apreensão no que diz respeito a segurança de dados, pois na visão de Rafael Taissun (2018):

> Você pode ter um dado que considera não sigiloso e que, nas mãos de qualquer pessoa, não representa um problema. Assim como é possível ter um dado que, em mãos erradas, poderia gerar grandes prejuízos para a organização, como formulas químicas de um produto ou senha utilizada na portaria eletrônica.

A segurança cibernética é uma realidade dentro das indústrias, e mesmo que haja preocupação por parte dos profissionais em virtude dos milhares de casos de ciberataques, a verdade é que ainda há muito o pensamento na cabeça dos gestores, que a empresa não será invadida (VENTURELLI, 2018), e por isso, relaxam no quesito de implementação de sistemas mais seguros para os seus negócios, assimilando-se ao dono da casa que deixa a porta aberta esperando o ladrão entrar.

Para Mário Venturelli(2018), as invasões aos sistemas ou dados estão ocorrendo em todo e qualquer seguimento, sem mesmo requerer por parte do invasor motivações para os cibercrimes, pois podem decorrem desde a simples satisfação pessoal do *hacker*, espionagem industrial, sequestro e bloqueio de dados, roubo das informações para futura chantagem, entre outros, eis que trata-se de um rol de motivos extenso.

Para o referido autor (VENTURELLI, 2018), há algumas características que tornam a fábrica vulnerável em questões de segurança, como:

(i) protocolos de baixa capacidade de segurança;
(ii) redes sem antivírus ou quando se encontram desatualizados;
(iii) sistemas operacionais sem atualização e com brechas conhecidas da TI;
(iv) redes de automação não são criptografadas no nível IP.

Esses são alguns exemplos, mas há outros defeitos na infraestrutrura de segurança, que permitem que os *hackers* de plantão invadam o sistema industrial.

Essa vulnerabilidade quanto àcibersegurança nos ambientes industriais é o que faz com que as empresas sejam as vítimas favoritas dos crimes cibernéticos, pois se tornam presas fáceis. E é nesse sentido que se encontra um dos maiores desafios da Indústria 4.0, os quais correspondem às redes, os processos e as operações inadequadamente protegidas, uma vez que se tenta conectar todos os elementos e partes interessadas em uma mesma cadeia produtiva (TELLIUM, 2017).

Isso porque, pelo fato das transformações tecnológicas serem tão grandes que quase é impossível de se conseguir acompanhar, quanto mais às conexões que são feitas, é como se desse passagem à criação de novos riscos à segurança também, não podendo assim, ficar esperando que surja o momento certo para começar a investir em tecnologias que visem a proteção do ambiente organizacional (STRATEC, 2019).

Para se verificar a que ponto tem chegado à capacidade dos invasores cibernéticos para coletar dados, cita-se o caso ocorrido nos Estados Unidos, em que um cassino foi invadido por *crackers* e teve mais de 10GB de dados roubados, através da

vulnerabilidade de um aquário que havia no estabelecimento. O aquário era conectado a um computador via *wi-fi,* pelo qual era controlada a temperatura da água dos peixes.

Através desse *software* os criminosos conseguiram acessar uma falha de segurança do dispositivo regulador, e por meio deste, conseguiram acessar a rede interna do cassino. Os dados roubados foram parar em algum lugar da Finlândia (OSTEC, 2019). Isso mostra o quanto às inovações tecnológicas podem ser surpreendentes e assustadoras ao mesmo tempo.

Com os diários casos de invasões cibernéticos, não se questiona mais se é importante investir em segurança, mas sim, como será esse investimento, para vencer esses desafios, o que é primordial.

Neste sentido, considerando o intenso fluxo de inovações tecnológicas, será preciso desenvolver mecanismos de defesa que sejam eficientes para elidir ao máximo qualquer espécie de ataque ou simples ameaça, pois para que as empresas sobrevivem à nova era digital, será necessário antes de tudo, avaliar a vulnerabilidade da própria fábrica antes de elaborar o planejamento de segurança (NETEYE, 2018). Após, será preciso criar sistemas de proteção, detecção e planos de recuperação de desastres, eis apesar das tradicionais ferramentas de seguranças utilizadas até aqui serem ainda consideradas indispensáveis, necessita-se com urgência que novas opções de defesa sejam apresentadas à indústria (TELLIUM, 2017).

Porém, de acordo com Márcio Venturelli (2018), traçar um plano de segurança cibernética é algo complexo, todavia, há passos iniciais a serem tomadas que já consistirão em uma segurança mínima no chão da fábrica, as quais podendo consistir em mecanismos de defesa compreendem em controles técnicos, os quais podem ser:

(i) Autenticação de usuários e equipamentos;
(ii) Controle de acesso – físico e lógico;
(iii) detecção de intrusão – física e lógica;
(iv) criptografia de dados;
(v) assinatura digital;
(vi) isolamento e/ou segregação de ativos;
(vii) varredura de vírus;
(viii) monitoramento de atividade sistema/rede;
(ix) segurança perimetral de planta;
(x) *backup* de dados, pois em caso de roubo ou sequestro de informações, será possível restaurá-los para retornar as atividades.

Por sua vez, há uma espécie de controle, chamado de controles processuais, os quais não correspondem aos mecanismos digitais em si, mas possuem um papel fundamental dentro da cibersegurança, que consiste no treinamento e educação dos colaboradores da fábrica.

A inserção no mercado de trabalho na Indústria 4.0 por si só, exige do profissional, que este se aperfeiçoe conforme o surgimento das inovações tecnológicas. Assim também deverá de ocorrer com aqueles que manipulam diretamente os dados. Será preciso educar e desenvolver treinamentos dos funcionários para ter maior controle sobre as informações e prevenir crimes cibernéticos.

Para Ricardo Gonçalves (2018), o principal motivo do vazamento de dados dentro da indústria, parte do próprio funcionário corporativo, o qual se encontra despreparado, com ausência de treinamento e problemas no processo operacional. Para o mesmo autor:

> Por isso que, quando falamos em segurança, é fundamental manter em total harmonia o tripé: pessoas, processos e tecnologia. Não basta que os processos e a tecnologia sejam efetivos se os usuários não estiverem cientes de como é importante proteger o ambiente corporativo.

Percebe-se que a segurança de dados pode ser explorada por diversos ângulos, porém muitos gestores repelem a aplicação dessas medidas ao focar nos custos que isso causará no seu bolso (A VOZ DA INDÚSTRIA, 2018):

> o investimento necessário para proteger todos os dados de uma organização é incalculável, por isso, precisamos investir de forma seletiva e focada, protegendo aquilo que é mais sensível e sigiloso.

Porém, o caminho da segurança não é único. Deve-se analisar o perfil de cada empresa e ver quais medidas serão exigidas para que haja um elevado grau de proteção, até mesmo para não despender muitos recursos financeiros, sendo que a implementação de simples métodos já seria suficiente. A esse exemplo, pode-se citar a inserção de normas e procedimentos, que estipulam quais colaboradores terão acesso a rede, bem como criar um plano estratégico para restauração do sistema em caso de eventual invasão(TELLIUM, 2017).

Infelizmente não há tecnologia suficiente para proteger por completo o sistema industrial. A cibersegurança virá de vários mecanismos, para defender os mais diferentes tipos de ameaça, pois com a era digital, a cada dia que passa as ameaças e

impactos na segurança tomam proporções cada vez maiores. Só o tempo dirá se as medidas que hoje se busca implementar, se serão capazes de ser considerada uma infraestrutura de segurança no mínimo aceitável para a proteção da empresa e de seus dados (OSTEC, 2019).

Porém, conforme a tecnologia for avançando, se criará ferramentas cada vez mais eficientes para serem utilizadas no campo da segurança da informação. Será preciso estar sempre acompanhando os novos mecanismos e tentando encaixá-los ao negócio de acordo com as suas peculiaridades, pois os investimentos feitos hoje são menores do que os prejuízos milionários causados pelos crimes praticados no ambiente virtual (LUCENA, 2017).

A humanidade nunca viveu tempos tão conturbados, como os que têm vivido no século XXI. Isto porque a atual revolução industrial traz consigo, as mudanças mais ousadas e radicais, alterando substancialmente o âmbito dos negócios e a vida em sociedade.

Referências bibliográficas:

A INDÚSTRIA 4.0 está associada ao uso da tecnologia em todos os processos. *In:* **A voz da indústria**. [S.l, 2018. <Disponível em: https://avozdaindustria.com.br/seguranca-de-dados-industria-4-0/>. Acesso em: 14 abr. 2019.

ALECRIM, Emerson. **O que é GDPR e que diferença isso faz para quem é brasileiro**. [S. l], 2018. Disponível em: <https://tecnoblog.net/245101/gdpr-privacidade-protecao-dados/>. Acesso em: 13 abr. 2019.

ALMEIDA, Eduardo. **O papel da segurança na Indústria 4.0.** [S.l], 2018. Disponível em: <http://cio.com.br/opiniao/2018/09/25/o-papel-da-seguranca-na-industria-4.0/>. Acesso em: 25 out. 2018.

BENTO, Beatrice Helena Silveira. **A nova lei de proteção de dados no Brasil e o general data protectionregulation da União Europeia.** [S.l], 2018. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI289555,11049-A+nova+lei+de+protecao+de+dados+no+Brasil+e+o+general+data+protection>. Acesso em: 13 abr. 2019.

BRASIL. **Lei nº13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 13 abr. 2019.

COMO criar um plano de proteção de dados na Indústria 4.0. In: **FISPAL TEC DIGITAL**. [S. l], 19 mar. 2019. Disponível em: <https://digital.fispaltecnologia.com.br/como-criar-um-plano-de-protecao-de-dados-na-industria-4-0/>. Acesso em: 27 maio 2019.

COSTA, Rodrigo Loureiro Machado da. **Empresas sob ataque hacker**. [S.l], 2017. Disponível em: <https://www.istoedinheiro.com.br/empresas-sob-ataque-hacker/>. Acesso em: 12 abr. 2019.

DEPOIS do vapor, da eletricidade e da computação digital. *IN:* **Tellium**. [S.l], 2017. Disponível em: <https://blog.telium.com.br/industria-4-0-precisamos-conversar-sobre-a-necessidade-de-seguranca-no-setor/>. Acesso em: 14 abr. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

GONÇALVES, Ricardo. **Indústria 4.0 e a segurança dos dados: como acompanhar a evolução tecnológica de maneira segura?** [S. l], 2018. Disponível em: <https://computerworld.com.br/2018/07/12/industria-40-e-seguranca-dos-dados-como-acompanhar-evolucao-tecnologica-de-maneira-segura/>. Acesso em: 27 maio 2019.

INDÚSTRIA 4.0 pela perspectiva da segurança cibernética. *In:* **NetEye**. [S.l], 2018. Disponível em: <http://www.neteye.co/blog/industria-4-0-e-seguranca-cibernetica/>. Acesso em: 10 abr. 2019.

LIMBERGER, Têmis. **O direito à intimidade na era da informática**. Porto Alegre: Livraria do Advogado, 2007.

LUCENA, Felipe. **Segurança de Dados: Tudo que você precisa saber**. [S.l], 2017. Disponível em: <https://blog.diferencialti.com.br/seguranca-de-dados/>. Acesso em: 15 abr. 2019.

MARTINS, Danylo. **Invasões cibernéticas criminosas ameaçam os negócios**. [S.l], 2018. Disponível em: <https://www.valor.com.br/financas/5552593/invasoes-ciberneticas-criminosas-ameacam-os-negocios%20>. Acesso em: 12 abr. 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor** – linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MOREIRA, André de Oliveira Schenini. **A lei de proteção de dados pessoais da União Europeia (GDPR) e sua aplicação extraterritorial às entidades e empresas brasileiras**. [S.l], 2017. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI267772,81042-A+lei+de+protecao+de+dados+pessoais+da+Uniao+Europeia+GDPR+e+sua>. Acesso em: 13 abr. 2019.

O mundo já passou por constantes transformações impactantes. *IN:* **Stratec**. [S.l, 2019?]. Disponível em: <https://www.stratec.com.br/blog/a-industria-4-0-e-os-desafios-da-gestao/>. Acesso em: 14 abr. 2019.

PEIXES em um aquário podemos ensinar muito sobre a importância da segurança de dados. *IN:* **OSTEC Blog**.[S.l, 2019?]. Disponível em: <https://ostec.blog/seguranca-perimetro/impactos-falhas-seguranca-iot>. Acesso em: 14 abr. 2019.

SANTI, Thais. **Segurança cibernética na Indústria 4.0.** [S.l], 2018. Disponível em: <http://www.revistaopapel.org.br/noticia-anexos/1519095872_ede2eddce57f23f22bea51a942bb5a2c_1523942224.pdf>. Acessoem: 10 abr. 2019.

SEGRAN, Elizabeth. **The Ethical Quandaries You Should Think About The Next Time You Look at Your Phone**. 2015. Disponível em: http://www.fastcompany.com/3051786/most-creative-people/the-ethical-quandaries-you-should-think-about-the-next-time-you-look-at. Acesso em: 25 out. 2018.

SENDO a tecnologia, conectada a uma rede. *In:* **Piramidal.** [S.l], 2018. Disponível em: <http://www.piramidal.com.br/blog/industria-4-0/como-funciona-a-seguranca-de-dados-na-industria-4-0/#>. Acesso em: 10 abr. 2019.

TELIUM. **Indústria 4.0! precisamos conversar sobre a necessidade de segurança no setor.** [S.l], 2017. Disponível em: <https://blog.telium.com.br/industria-4-0-precisamos-conversar-sobre-a-necessidade-de-seguranca-no-setor/>. Acesso em: 25 out. 2018.

VENTURA, Leonardo Henrique de Carvalho. **Considerações sobre a norma europeia de proteção de dados – GDPR.** [S.l], 2018. Disponível em: <https://jus.com.br/artigos/69969/consideracoes-sobre-a-norma-europeia-de-protecao-de-dados-gdpr>. Acesso em: 14 abr. 2019.

VENTURELLI, Márcio. **O futuro do emprego na Indústria 4.0**. [*S.l*], 29 maio 2018. Disponível em: <https://www.automacaoindustrial.info/o-futuro-do-emprego-na-industria-4-0/>. Acesso em: 14 abr. 2019.