O IMPLANTE DE CHIP EM TRABALHADORAS E TRABALHADORES: AS VICISSITUDES DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) BRASILEIRA E DA *GENERAL DATA PROTECTION REGULATION* (GDPR) EUROPEIA

Sheila Stolz[*]
Manuel Martín Pino Estrada[**]

RESUMO

O implante de chip em trabalhadoras(es) tem como diretriz ético-jurídica o consentimento livremente manifestado, única forma de capaz de salvaguardar, segundo as normativas legais brasileiras e europeias que serão analisadas no decorrer deste ensaio, as questões pertinentes a privacidade e a intimidade. Não obstante, considerando-se que através dos chips os empregadores poderão saber *on line* e *full time* a localização de suas(seus) subordinadas(os) e, também, monitorar continuamente a sua saúde – posto que terão acesso, por exemplo, à pressão sanguínea, o ritmo da respiração e dos batimentos cardíacos – convém realizar-se a pergunta: a implantação do chip não extrapola o poder de direção do empregador? Salienta-se, ademais, que a exigência prevista nas normativas legais mencionadas de que o

[*] Professora Associada do Curso de Direito e do Programa de Pós-Graduação em Direito e Justiça Social (Mestrado) da Universidade Federal do Rio Grande (FaDir/FURG/RS). Doutora em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC/RS), com bolsa do Programa de Doutorado Sanduíche no Exterior (PDSE-CAPES) realizado na *Facultad de Derecho* da*Universidad Complutense de Madrid* (UCM/Madri/Espanha). Mestre em Direito pela *Universitat Pompeu Fabra* (UPF/Barcelona/Espanha). Coordenadora Geral do Núcleo de Pesquisa e Extensão em Direitos Humanos (NUPEDH/FURG). Coordenadora da especialização em Educação em Direitos Humanos (PGEDH/FURG-UAB-CAPES).

[**] Professor de Direito do Trabalho, Direito Digital e de Inteligência Artificial na Escola Superior de Advocacia (ESA) da OAB/SP. Membro do Conselho Consultivo e Fiscal do Instituto Direito e Inteligência Artificial (IDEIA). Formado em Direito na Universidade de São Paulo (USP), Mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS) e doutorando em Direito na Faculdade Autônoma de Direito de São Paulo (FADISP).

consentimento das(os) trabalhadoras(es) pressupõe como válida a aceitação do implante do chip, não toma em consideração que este instrumento (consentimento) não reflete a plena autonomia e liberdade das pessoas que trabalham, pois o consentimento não é um mecanismo hábil a salvaguardar este polo da relação laboral que não dispõem de poder de negociação e transação, menos, ainda, de manifestar-se livremente em um contexto de flexibilização laboral inaugurado pela Reforma Trabalhista (LEI Nº 13.467 de 13 de julho de 2017), de colapso político-econômico agravado pela crise sociosanitária provocada pela pandemia do Vírus SARS-CoV-2/COVID-19, temáticas que serão discutidas neste ensaio.

PALAVRAS-CHAVE: Direito do Trabalho. Privacidade e Intimidade. Implante de Chip em Trabalhadoras(es).

THE CHIP IMPLANT IN WORKERS: THE REGULATORY VACUUMS OF THE BRASILIAN GENERAL DATA PROTECTION REGULATION LAW (LGPD) AND THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR)

ABSTRACT

The implantation of a chip in workers has as its ethical-legal guideline the consent freely expressed, the only way to decide, according to the Brazilian and European legal norms that will be analyzed in the course of this essay, the pertinent issues of privacy and intimacy. However, considering that through the chips, employers will be able to know online and full time the location of their subordinates and, continuously monitor your health – since they will have access, for example, to blood pressure, breathing rate and heart rate – the question should be asked: does the implantation of the chip not exceed the employer's power of direction? It should also be noted that the consent expressed by workers presupposes the acceptance of the chip implant as valid, does not take into account that this instrument (consent) does not reflect the full autonomy and freedom of the people who work, as consent is not a sufficiently skillful mechanism to safeguard the rights of workers who do not have the power to negotiate, even less, to express themselves freely in a context of labor flexibility inaugurated by the Labor Reform (Act Nº 13.467 of July 13, 2017), political and economic collapse aggravated by the socio-health crisis caused by the SARS-CoV-2/COVID-19 Virus pandemic, themes that will be discussed in this essay.

KEYWORDS: Labor Law. Privacy and Intimacy. Chip Implant in Workers.

INTRODUÇÃO

Tal é a preeminência das inovações científicas e de tecnologias da informação e da comunicação que nosso momento histórico tem sido autodenominado como a Era da Informação Tecnológica (CASTELLS, 2000) ou, também, como a Era do Mundo Digital. No entanto, estas não são as únicas alterações que as sociedades atuais experimentam, pois estão sujeitas a uma multiplicidade de transformações que moldam tanto a forma como se organizam como também os diferentes tipos de relacionamentos que dentro dela ocorrem (TEZANOS, 2002). Desde a perspectiva do Direito ao/do Trabalho dois processos adicionais de mudança têm se destacado, a saber: a globalização da economia e das finanças, por um lado, e a expansão da ideologia neoliberal, por outro; e, com eles, inúmeros são os impactos que as relações trabalhistas vêm sofrendo (ARTHURS, 2006). No que concerne ao foco de análise deste ensaio, o pano de fundo deste cenário está emoldurado por uma profunda alteração das relações de poder – mudanças aqui entendidas em sentido amplo, não apenas legal – que vêm sendo paulatina e tendenciosamente pendentes em prol de favorecer os interesses exclusivos das empresas, ignorando, desta forma, a finalidade precípua do Direito do Trabalho que tradicionalmente consistia em proteger a parte mais débil da relação de trabalho/emprego e, particularmente, em salvaguardar os direitos fundamentais das pessoas que trabalham (STOLZ, 2018 e 2014).

O controle das pessoas através do uso de seus dados vem se expandindo vertiginosamente e, no meio empresarial (GOLDSMITH; WU, 2006), tornou-se uma obsessão, pois a manipulação do comportamento humano é uma importante forma de poder seja, por exemplo, para influenciar hábitos de consumo, como também para determinar o resultado de eleições democráticas. O implante de chip em trabalhadoras e trabalhadores, todavia não foi adotado no Brasil, mas não restam dúvidas que a inserção de um objeto dentro de seus corpos, mesmo que para fins exclusivos do empregador, é algo polêmico.

Com o objetivo de compreender o tema em tela de debate, a estratégia metodológica adotada foi a de pesquisar tanto em âmbito europeu como nacional, a bibliografia e as legislações pertinentes.

Outrossim, o ensaio a seguir se subdivide, em um primeiro momento, no estudo e na apresentação sistemática do que são os tipos de dados e de sistemas de dados para, a partir deste enfoque, entender por onde navegam estes dados, tema que corresponde a segunda seção. A terceira seção demonstrará que os dados da pessoa natural possuem imenso valor no mercado e, precisamente por isto, a necessidade de que se fiscalizem e controlem as informações que circulam nas redes e sistemas de dados. Esta seção está conectada as duas últimas que tratam do consentimento da pessoa natural no que concerne ao acesso e ao manuseio de seus dados, assim como em sua autorização expressa para o implante de chip pelo empregador/empresa quando estas pessoas estão desempenhando suas funções laborativas.

1. OS DADOS E OS SEUS TIPOS

Ainda que para a avassaladora maioria das(os) estudantes de Direito e profissionais da área jurídica só existam um tipo de dados, a saber: aqueles que tratam da identificação das pessoas – Registro Geral e CPF –, do *status* de trabalho e/ou da profissão exercida – carteira de trabalho, PIS/PASEP, registro no INSS, registro na OAB, no CREA, entre outros –, ou que dizem respeito a sua moradia – endereço residencial –, dados que são fáceis de encontrar nos buscadores existentes e que tanto o mercado lícito e ilícito de dados têm a seu dispor, muitos outros dados existem sobre as pessoas físicas.

1.1 Dados pessoais

Segundo a Lei Geral de Proteção de Dados (LGPD) nº 13.709/18, no art. 5º, inciso I, dados pessoais são as informações relacionadas "a pessoa natural identificada ou identificável"[1].

Neste caso, trata-se do conjunto de dados de fácil acesso, tais como o nome, endereço, RG, CPF, local de trabalho e afins.

[1] Brasil. **Lei Geral de Proteção de Dados (LGPD) nº 13.709/18**. Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 de mar. 2020.

1.2 Dados locacionais

Segundo o inciso I do art. 14 do Decreto nº 8.771/2016, os dados locacionais são dados pessoais referentes à localização geográfica da pessoa física ou natural, em conjunto com o entendimento do § 1º do art. 11 do Marco Civil da Internet (Lei nº 12.965/2014).

1.3 Dados sensíveis

Estes dados são considerados mais importantes, pois de natureza íntima e privativa da pessoa natural. Segundo a LGPD, no art. 5º, inciso II, os dados sensíveis são aqueles referentes a pessoa e dizem respeito a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Continuando a normatizar a LGPD, o Decreto nº 10.046 de 9 de outubro de 2019, em seu no art. 2º, inciso II define o que são "dados biométricos", como aqueles dados que estão dentro do âmbito dos "dados sensíveis" da Lei em questão, definindo-os como: "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar"[2].

Percebe-se que o conceito de dado biométrico é mais abrangente que a noção de impressão digital, pois integra as características pessoais, como, por exemplo, a voz e a maneira de andar de uma pessoa e que são dados que podem ser colhidos usando as novas tecnologias de reconhecimento facial.

O próprio Decreto nº 10.046, em seu art. 2º, inciso IV menciona o que é um "atributo genético", que está dentro da definição de "dados sensíveis", mencionado pela própria LGPD: "características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas".

[2] Brasil. **Decreto Nº 10.046, de 9 de Outubro de 2019**. Brasília: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 20 de mar. 2020.

Salienta-se que, o Decreto em questão, em seu artigo 1º, trata do compartilhamento destes dados entre os "órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União", tendo como um dos objetivos a criação de "políticas públicas", e que, segundo o art. 11, inciso II, alínea "b)" da LGPD, o recolhimento destes dados pela administração pública **dispensa a autorização da pessoa física** por também configurarem uma questão de "política pública" (grifos da autora e do autor do artigo).

Ressalta-se que existem mais dados que o Governo Federal tem controle, conforme o Decreto nº 10.047 de 9 de outubro de 2019 que criou o Cadastro Nacional de Informações Sociais (CNIS) e onde estabelece, no art. 3º, I, que o Instituto Nacional do Seguro Social (INSS) é o órgão encarregado de administrá-lo, tendo este cadastro 51 (cinquenta e uma) bases de dados, que incluem, entre outros, o Cadastro Nacional de Pessoa Jurídica (CNPJ), o Programa Volta para Casa (PVC), o Sistema de Informação do Câncer do Colo do Útero (SISCOLO), o Sistema de Cadastro de Usuários do SUS (CADSUS) e o Sistema Águia (Receita Federal), por exemplo.

1.4 Dado anonimizado

Segundo o inciso III do art. 5º da LGPD, é um dado relativo ao titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

1.5 Dados de conexão

Segundo o inciso I do § 1º do art. 10-A da Lei nº 12.850 de 2013[3], os dados de conexão são informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e do terminal de origem da conexão.

[3] BRASIL. **Lei nº 12.850 de 2013**. Brasília: Congresso Nacional, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em 15 de abr. 2020.

1.6 Dados cadastrais

De acordo com o inciso II do § 1º do art. 10-A da Lei nº 12.850 de 2013 os dados cadastrais são informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem o endereço de IP, a identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.

1.7 Dados processados

A Portaria nº 93 de 26 de setembro de 2019 que consiste em um glossário de Direito Digital, determina que os dados processados são aqueles dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação. Convém destacar que todos os dados sejam eles pessoais, locacionais, de conexão, entre tantos outros, são dados processados.

1.8 Metadados

Os metadados são pouco tratados dentro do ambiente da LGPD, sendo obviamente protegidos por esta Lei, cuja definição, conforme a Portaria nº 93 de 26 de setembro de 2019 representam os "dados sobre dados" e aprovisionam os "recursos necessários para entender os dados através do tempo, ou seja, são dados estruturados que fornecem uma descrição concisa a respeito dos dados armazenados e permitem encontrar, gerenciar, compreender ou preservar informações a respeito dos dados ao longo do tempo"[4].

A expressão "dados sobre dados" se refere aos dados produzidos através do cruzamento de dados entre bases de dados, assim como aos gráficos, documentos, tabelas, fotos, imagens, vídeos, entre outros, que acabam ministrando dados específicos quando há uma análise detalhada destes.

[4] BRASIL. **Portaria nº 93 de 26 de setembro de 2019**. Brasília: DOU, 2029. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em 19 de abr. 2020.

1.9 Banco de dados

A Portaria nº 93 de 26 de setembro de 2019, estabelece que se configura um banco de dados quando há uma coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam de forma a criar algum sentido sobre as informações coletadas possibilitando mais eficiência durante uma consulta e gerando novos e mais conhecimentos correlacionados a respeito de determinados dados, situações, contextos.

1.10 Megadados

O aumento exponencial da disponibilidade e da utilização automatizada de informações gera os megadados – conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grandes dimensões que são extensivamente analisados com recursos a algoritmos informáticos.

2. ONDE NAVEGAM OS DADOS?

Os dados navegam na Internet, tanto superficial, quanto na profunda e na escura, incluindo os mundos virtuais, cuja explicação será desenvolvida nesta seção, mas a coleta dos mesmos e o seu manuseio encontram-se protegidas pela Lei Geral de Proteção de Dados (LGPD), ainda que na prática dita proteção é limitada.

2.1 A Internet superficial, profunda e escura

Os dados que atualmente navegam na Internet superficial, representam somente 0,15% da Internet total e nesta as(os) usuárias(os) leigas(os) são rastreadas(os) e monitoradas(os) o tempo todo, diferentemente do que ocorre na Internet profunda que representa 99,85% de toda a Internet, livre de censura e de difícil monitoramento e rastreamento. A Internet profunda costuma ser relacionada pelos meios de comunicação social, o Governo Federal e as empresas privadas aos crimes digitais, o que de fato não corresponde a definição legal deste tipo de crime que se configura, por

exemplo, quando os e-mails, *Whatsapps*, *Facebooks*, *Instagrams*, telefones celulares são invadidos por terceiras pessoas sejam elas físicas ou jurídicas (tais como as agências estadunidenses de espionagem que possuem filiais no Brasil e/ou mesmo as agências governamentais brasileiras e empresas nacionais ou transnacionais).

Dentro da Internet profunda está a escura, onde acontecem os crimes informáticos, ou seja, partem daqui as invasões de contas bancárias e de e-mails, por exemplo. E é também neste domínio que se encontram os sites de pedofilia, de tráfico, escravização e venda de pessoas e de órgãos humanos, de armamento bélico pesado e de armas químicas; todo um rol de "produtos e serviços" que, se fossem oferecidos na Internet superficial, seriam facilmente interceptados, motivo pelo qual encontram-se nas profundezas da Internet facilmente ocultados e muito prósperos em seus negócios ilícitos.

2.2 Mundos virtuais

Consistem naqueles mundos onde os usuários usam "avatares", sendo estes uma espécie de "bonecos" virtuais em três dimensões que navegam num mundo também em três dimensões, e aqui encontram-se as lojas, empresas nacionais e multinacionais (como a IBM, por exemplo), Tribunais, universidades, embaixadas, consulados, centros de pesquisas, assim, como as redes de supermercados, restaurantes, boates, estádios e lugares de concerto de música, tanto que existem artistas que apenas são conhecidos nos mundos virtuais e não no mundo físico. Entre os mundos virtuais os mais notórios são o *Second Life*, o *Kaneva* e o *There*. Obviamente que nestes mundos virtuais o rol de dados mencionados navega facilmente, pois não há dúvidas de que o comportamento humano configura um dado de fundamental interesse tanto para as empresas como para os governos.

2.3 O "fatiamento" da pessoa natural em centenas de dados que valem muito dinheiro

A imensa maioria das pessoas pensam que seus dados se resumem ao RG e ao CPF, mas estão totalmente erradas, afinal, o nosso comportamento é um dado muito importante, mas este comportamento também é "fatiado" em muitos dados

comportamentais específicos, tais como, a forma de andar, o jeito de manusear o *mouse*, a nossa forma de olhar, de rir, de chorar, de ficar triste, de ajoelhar, de pensar e assim por diante, mas, obviamente, não é só isso, as empresas privadas e públicas e também os governos federal, estaduais, municipais e distrital querem mais informações sobre as pessoas tais como o batimento cardíaco, o histórico genético, a forma de respirar, as reações quando encontramos alguém ou vemos alguma propaganda, as preferências sexuais, alimentícias e de consumo.

Outros dados relevantes, além dos supracitados, são, por exemplo, aqueles concernentes ao funcionamento do fígado, do rim, do pâncreas, da bexiga, da próstata, do pulmão, do estômago, o estado dos ossos, dos músculos, dos ligamentos, da pele das pessoas, assim como o estado da visão e da audição. Dados que são alimentados 24 (vinte e quatro) horas por dia, durante os 365 (trezentos e sessenta e cinco) dias do ano, mas mesmo com todas estas informações, as empresas privadas e públicas e os governos do mundo inteiro querem saber como as pessoas pensam o tempo todo, o dia inteiro, ou seja, querem chegar aos pensamentos mais íntimos da pessoa, invadir seu cérebro e seu comportamento. Salienta-se que as relações familiares, interpessoais e também as financeiras são monitoradas e documentadas *full time*.

Então, a LGPD não consegue proteger os dados pessoais, sensíveis e os metadados, isso é uma utopia, pois as pessoas são monitoradas e rastreadas o tempo inteiro, fato real do qual não se pode elidir – o recente caso do Estado de São Paulo que firmou acordo com operadoras de celular para monitorar o lockdown e, posteriormente, o isolamento e o distanciamento social ampliado e seletivo necessários para o enfrentamento da pandemia do novo Corona vírus (Sars-CoV-2[5]) e a respectiva doença por ele provocada (COVID-19 – *Corona*

[5] Segundo a FIUCRUZ: "os coronavírus causam infecções respiratórias em seres humanos e em animais. Geralmente, são doenças respiratórias leves a moderadas, semelhantes a um resfriado comum. Já o novo coronavírus é uma nova cepa do vírus (2019-nCoV) que foi notificada em humanos pela primeira vez na cidade de Wuhan, na província de Hubei, na China". Disponível em: <https://portal.fiocruz.br/pergunta/o-que-e-o-novo-coronavirus>. Acesso em 3 de jun. de 2020.

Virus Disease de 2019), é um vívido exemplo[6].

3. A DESNECESSIDADE DO CONSENTIMENTO DA PESSOA NATURAL PARA O ACESSO AOS SEUS DADOS SENSÍVEIS

O consentimento, segundo o art. 5º, inciso XII da LGPD é uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Neste caso, o titular do dado, que é a pessoa física, concorda em entregar os seus dados, mas, obviamente, a pessoa física também tem o direito de não querer entregá-los, ou seja, a normativa preserva o direito de que a pessoa física não forneça os seus dados pessoais e sensíveis se assim o desejar. Não obstante, esta não é uma afirmação que possua equivalência com a realidade, pois, o art. 4º da LGPD trata das hipóteses da não aplicação de tal direito, especificamente em seu inciso III a seguir descrito:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado.

Salienta-se que, no caso destas hipóteses, o Governo Federal poderá acessar toda a vida da pessoa natural sem o seu consentimento, ou seja, o direito fundamental à privacidade fica totalmente sem amparo legal.

Existem também outras hipóteses, como é o caso do art. 11, inciso II, alínea "b)" da própria LGPD, que permite a invasão e o acesso (de forma específica) aos dados sensíveis, normativa que em conjunto com os Decretos nº 10.046 e 10.047 de 9 de setembro de 2019 conformam muito mais do que um simples acesso ao código genético, a íris dos olhos e à vida sexual das pessoas naturais, tal qual

[6] Notícia veiculada publicamente. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2020/04/09/sp-fechou-acordo-com-operadoras-de-celular-para-monitorar-isolamento-diz-doria.htm?fbclid=IwAR0Bcwql2P5RrVhQAwpTs5wM0EYNMTqEGnUS6VEbrSDROZqAIrFLQqGufrc Acesso em 09 abr. 2020.

se deduz da leitura do referido artigo:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.

Neste caso, tendo em vista o desenvolvimento de "políticas públicas", os dados sensíveis – que são os mais importantes por serem íntimos da pessoa natural – são os que poderão ser acessados e manuseados à vontade pela administração pública. E, convém recordar que no âmbito da Lei nº 12.850/2013, existe a possibilidade de acesso aos dados da pessoa natural pelo delegado de polícia e pelo Ministério Público, independentemente de autorização judicial, conforme estipulado nos artigos *in verbis*:

> Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradoras de cartão de crédito.
> Art. 16. As empresas de transporte possibilitarão, pelo prazo de 5 (cinco) anos, acesso direto e permanente do juiz, do Ministério Público ou do delegado de polícia aos bancos de dados de reservas e registro de viagens.

Conforme argumentado, são muitas informações que o titular dos dados disponibiliza sem o seu consentimento. Recordando que, nos processos de investigação e até que se eliminem as suspeitas, qualquer pessoa física pode ser tratada como suspeita e, portanto, ter seus dados investigados. Para concluir esta seção, convém frisar que cotidianamente, através do uso das câmeras de vigilância (nos aeroportos e metrôs, por exemplo) que dispõem de dispositivos de reconhecimento facial, os dados sensíveis estão sendo acessados sem consentimento algum das pessoas.

4. O IMPLANTE DE CHIP NAS(OS) TRABALHADORAS(ES) NO ÂMBITO EUROPEU E BRASILEIRO

4.1 O implante de chip segundo a *General Data Protection Regulation* (GDPR/União Europeia)

Na União Europeia, a *General Data Protection Regulation* (Regulamentação de Proteção de Dados da União Europeia - GDPR) datada de 2018 e em vigor (normativa que inspira a LGPD brasileira), define o consentimento como:

> Art. 4º: Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Dita definição serve como base para o implante de chip pelas empresas em suas(seus) trabalhadoras(es), ou seja, caso a pessoa consinta que lhe seja implantado este aparelho em seu corpo, não haverá nenhum obstáculo legal que impeça esta ação, pois existe um regulamento da União Europeia que trata de regulamentar este tema.

Um empregador/empresa que confia no consentimento para processar dados pessoais de suas(seus) trabalhadoras(es) deve satisfazer os seguintes requisitos da Regulamentação de Proteção de Dados da União Europeia (GDPR), a saber:

1. O consentimento deve ser específico e informado, incluindo informações sobre o direito de retirar o consentimento.
2. O consentimento deve ser dado livremente.
3. O consentimento deve ser inequívoco e assumir a forma de uma ação afirmativa ou declaração.
4. Para certos tipos de processamento de dados pessoais, o consentimento deve ser explícito.
5. Quando o consentimento é dado em um documento que também diz respeito a outros assuntos, a solicitação para o consentimento, deve ser:
   - Apresentada de maneira claramente diferenciada dos outros assuntos.
   - Ser inteligível e facilmente acessível.

- Estar redigida em linguagem clara e objetiva.

6. A(O) trabalhadora(trabalhador) individual necessariamente deve ser informada(o) e dar seu consentimento sobre os usos a que se destinam as informações colhidas pelo chip implantado, incluindo a divulgação de tais dados e o compartilhamento com terceiros[7].

Qualquer falha no cumprimento de tais requisitos equivaleria a uma violação da Lei, sendo permitido a(o) trabalhadora(trabalhador) reivindicar compensação equivalente a infração de direitos. Como observado acima, mesmo nos casos em que a implantação é dada de forma voluntária, as aplicações do uso de chip podem aumentar o potencial de problemas de proteção de dados, mais ainda se tal uso for estendido e utilizado, por exemplo, por outro empregador/empresa ou por mais de um empregador/empresa (no caso, por exemplo, das atividades terceirizadas que servem a mais de uma contratação de mão de obra). Considerações semelhantes também serão aplicadas no caso de usos não relacionados ao local de trabalho, como por um clube e/ou ginásio esportivo.

No que concerne a LGPD, a definição de consentimento nela explicitada, permite que se implantem chips nas(os) trabalhadoras(es) o que permitirá ao empregador controlar suas(seus) subordinadas(os) 24 (vinte e quatro) horas por dia, pois estes chips têm geolocalizadores que repassam, além da localização das pessoas, dados referentes, entre outros, a pressão sanguínea e aos batimentos cardíacos. Recordando que em um país como o Brasil com altos índices de desemprego e de trabalho informal, acreditar que o consentimento será plenamente livre e não viciado, não parece ser uma asserção nada compatível com a realidade.

[7] UNIÃO EUROPEIA. **Directorate General for Internal Policies**: The Use of Implant for Workers. Disponível em: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/614209/IPOL_STU(2018)614209_EN.pdf. Acesso em 12 fev. 2020.

4.2 Os chips ou "identificadores por rádio frequência" no âmbito da União Europeia

A identificação por radiofrequências (sigla "RFID" em inglês) consiste em uma tecnologia que permite a identificação e captação de dados de forma automática mediante a utilização de radiofrequência. Esta tecnologia tem como principal característica permitir associar um identificador único e outras informações recorrendo a uma *micropastilha* (chip) a ser inserida em qualquer objeto, animal ou mesmo pessoa e, através dela, ler as informações geradas mediante um dispositivo sem fios. Os dispositivos RFID são além de "etiquetas electrónicas" e/ou "códigos de barras electrónicos", dispositivos ligados a bases de dados e a redes de comunicações, como a Internet e, sendo assim, convém recordar que esta tecnologia proporciona um poderoso modo de oferta de novos serviços e aplicações, praticamente em qualquer ambiente.

Os dispositivos RFID são, na verdade, vistos como a porta de entrada para uma nova fase de desenvolvimento da sociedade da informação (termo utilizado por CASTELLS; CARDOSO, 2006), muitas vezes denominada "Internet das coisas", na qual a Internet interliga não só computadores e terminais de comunicações, como, potencialmente, qualquer dos objetos que nos rodeiam todos os dias – vestuário e outros bens de consumo, por exemplo. Não restam dúvidas de que tais dispositivos possam servir para violar direitos fundamentais e, entre eles, os de privacidade, bem como poderão originar discriminações, práticas de exclusão e mesmo a perda do emprego e/ou trabalho.

É claro que a aplicação da RFID deve ser social, jurídica e politicamente aceita e regulada, mas, sobretudo, eticamente guiada. A RFID só poderá proporcionar os seus inúmeros benefícios econômicos e sociais se houverem garantias efetivas relativas à proteção dos dados e da privacidade e à correspondente dimensão ética que está no centro do debate sobre a aceitação pública da RFID. A proteção dos dados pessoais constitui um princípio importante na UE. O artigo 6° do Tratado da União Europeia declara que a União se fundamenta nos princípios da liberdade, da democracia, do respeito aos Direitos Humanos e as liberdades fundamentais; o artigo 30° exige a adopção de disposições adequadas relativas à proteção dos dados pessoais no

que respeita à coleta, armazenamento, tratamento, análise e intercâmbio de informações no domínio da cooperação policial. A proteção dos dados pessoais é consagrada como uma das liberdades no artigo 8° da Carta Europeia dos Direitos Fundamentais.

No domínio da saúde, a Comunidade Europeia, há muito tempo monitoriza, com o apoio dos seus comités científicos, os eventuais efeitos dos campos eletromagnéticos (CEM) na saúde humana, estando em vigor um quadro jurídico que protege as(os) trabalhadoras(es) e amplamente a cidadania. Este quadro recomenda limites para a exposição da população a CEM (Recomendação 1999/519/CE, atualmente em revisão) e impõe regras estritas para a exposição das(os) trabalhadoras(es) (Diretiva 2004/40/CE) a estas emissões. Além destas normativas, foram estabelecidas restrições às emissões eletromagnéticas de produtos presentes no mercado Europeu, para garantir a segurança de utilizadores e não-utilizadores dos mesmos (Diretiva 1999/5/CE). Em geral, a intensidade dos CEM associados às aplicações RFID é baixa. Espera-se que nestes casos, e em condições normais de funcionamento, a exposição da população e das(os) trabalhadoras(es) aos CEM associados aos dispositivos RFID seja muito inferior aos limites atualmente em vigor. No entanto, se estima que a implantação dos dispositivos RFID seja acompanhada pelo crescimento generalizado das aplicações sem fios (televisão móvel, televisão digital, banda larga sem fios, etc.)[8].

4.3 A Diretiva 2004/40/CE sobre prescrições mínimas de segurança e saúde em matéria de exposição das(os) trabalhadoras(es) aos campos eletromagnéticos

A presente Diretiva estabelece as prescrições mínimas em matéria de proteção à saúde das pessoas que trabalham e tem como finalidade evitar os riscos a saúde que há exposição a campos eletromagnéticos (0 Hz-300 GHz) possa ocasionar, pois existem

[8] COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITE ECONÔMICO E SOCIAL EUROPEU E AO COMITE DAS REGIÕES. **Identificação por radiofrequências (RFID) na Europa**: rumo a um quadro político. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:PT:HTML. Acesso em 15 fev. 2020.

efeitos prejudiciais conhecidos e que se manifestam a curto prazo no corpo humano, causados pela circulação de correntes induzidas e pela absorção de energia, bem como pelas correntes de contato. Neste sentido, o art. 2º da Diretiva fornece várias definições importantes, são elas:

> a) Campo eletromagnético: qualquer campo magnético estático ou qualquer campo eléctrico, magnético ou eletromagnético variável no tempo com frequências até 300 GHz;
> b) Valores-limite de exposição: limites relativos à exposição a campos eletromagnéticos baseados diretamente em efeitos sobre a saúde já estabelecidos e em considerações biológicas. A observância destes limites garantirá a proteção dos trabalhadores expostos a campos eletromagnéticos contra todos os efeitos prejudiciais conhecidos para a saúde;
> c) Valores que desencadeiam a ação: magnitude de parâmetros diretamente mensuráveis, fornecidos em termos de intensidade do campo eléctrico (E), intensidade do campo magnético (H), densidade do fluxo magnético (B) e densidade de potência (S), a partir da qual devem ser tomadas uma ou mais das medidas especificadas na presente diretiva. A observância destes valores garantirá a observância dos valores-limite de exposição aplicáveis.

O nível de exposição aos campos eletromagnéticos pode ser reduzido mais eficazmente pela adopção de medidas preventivas desde a fase de concepção dos postos de trabalho e dos locais de trabalho, bem como pela escolha do equipamento de proteção e dos processos e métodos de trabalho, de modo a reduzir, prioritariamente, os riscos na origem. As disposições relativas aos equipamentos de proteção e aos métodos de trabalho contribuem para o resguardo das(os) trabalhadoras(es) envolvidas(os), além disto, as entidades patronais devem adaptar-se ao progresso técnico e aos conhecimentos científicos em matéria de riscos vinculados à exposição a campos eletromagnéticos, com vistas a melhorar a proteção da segurança e da saúde das(os) trabalhadoras(es).

No cumprimento das obrigações constantes do nº 3 do artigo 6º e do nº 1 do artigo 9º da Diretiva 89/391/CEE, a entidade patronal deve avaliar e, se for caso, medir e/ou calcular os níveis dos campos eletromagnéticos a que as(os) trabalhadoras(es) se encontram

expostas(os). A avaliação, a medição e o cálculo poderão, até à adopção de normas europeias harmonizadas do Cenelec[9], ser efetuadas em conformidade com as normas e/ou orientações científicas a que se refere o artigo 3º, levando em consideração, ademais, os níveis de emissão fornecidos pelos fabricantes do equipamento quando este esteja abrangido pelas diretivas comunitárias aplicáveis.

Segundo o nº 5 do artigo 4º da Diretiva 2004/40, a entidade patronal deve, ao proceder à avaliação dos riscos, prestar especial atenção aos seguintes elementos:

> a) Nível, espectro de frequência, duração e tipo de exposição;
> b) Valores-limite de exposição e valores que desencadeiam a ação referidos no artigo 3º da presente diretiva;
> c) Efeitos sobre a saúde e a segurança dos trabalhadores expostos a riscos especiais;
> d) Efeitos indiretos, tais como:
> i) a interferência com equipamentos e instrumentos médicos electrónicos (incluindo estimuladores cardíacos e outros implantes),
> ii) o risco de projeção de objetos ferromagnéticos em campos magnéticos estáticos com uma densidade de fluxo magnético superior a 3 mT,
> iii) o arranque de aparelhos eletro-explosivos (detonadores),
> iv) os incêndios e as explosões resultantes da inflamação de materiais inflamáveis devida a faíscas originadas por campos induzidos, correntes de contato ou descargas de faíscas;
> e) Existência de equipamentos de substituição concebidos para reduzir os níveis de exposição a campos eletromagnéticos;
> f) Informações adequadas recolhidas em resultado da vigilância da saúde, incluindo as publicadas, na medida do possível;
> g) Fontes múltiplas de exposição;
> h) Exposição simultânea a campos de frequência múltipla.

Cabe ao empregador/empresa, portanto, zelar pela saúde das pessoas que trabalham quando as mesmas estão expostas às frequências eletromagnéticas, salientando que, tanto as regras do

[9] Comitê Europeu de Normalização Eletrotécnica ou o CENELEC – Comitê que prepara as normas relativas à eletricidade e a eletrônica para os países que pertencem à União Europeia. Disponível em: https://www.cenelec.eu/. Acesso em 15 fev. 2020.

Comitê Econômico e Social Europeu como as estipuladas pela Diretiva 2004/40 visam a proteção das pessoas, sobretudo, quando houver a necessidade de implantação de chips e/ou eventual trabalho em local onde a espectro das frequências são uma constante.

4.4 A possibilidade legal do implante de chip nas(os) trabalhadoras(es) no âmbito da Lei Geral de Proteção de Dados (LGPD)

De acordo com o artigo 5º, inciso XII, da LGPD, que trata do "consentimento", pode-se arguir que a(o) trabalhadora(trabalhador) podem consentir com o implante de um chip em seu corpo. Não obstante, o ponto crucial de questionamento reside no consentimento, isto é, na possibilidade de que o mesmo seja viciado, por exemplo, pela necessidade de manutenção e/ou ascensão no/do posto de trabalho ou, simplesmente, porque é um requisito indispensável para a admissão laboral.

O artigo 7º da LGPD autoriza que a(o) trabalhadora(trabalhador) possa também consentir no manuseio de seus dados pessoais e, a qualquer tempo, segundo o § 5º do artigo 8º, revogar dita permissão. Neste caso persiste o questionamento anterior, ou seja, esta garantia legal pode ser efetivamente requerida pela(o) trabalhadora(trabalhador) sem que sofra ameaças de rebaixamento, remanejo e demissão, por exemplo. Salienta-se que, conforme os artigos 15 e 16 da Lei Geral de Proteção de Dados, os dados das(os) trabalhadoras(es) serão eliminados pelo empregador/empresa após o fim do objeto dos mesmos (contrato de trabalho), porém, sua conservação é autorizada até que não se aplique mais sua utilização por questões judiciais.

CONCLUSÃO

O implante de chip nas(os) trabalhadoras(es) é normatizado pela União Europeia através da Regulamentação Geral de Proteção de Dados (GDPR) e tem, como fundamento, o consentimento livremente manifesto. No Brasil, a Lei Geral de Proteção de Dados (LGPD) que entrou em vigor no passado mês de agosto de 2020, na esteira da GDPR, também admite esta possibilidade.

Não obstante a admissibilidade jurídica, questiona-se a pertinência ética e de garantia dos direitos fundamentais envolvidos, pois, não restam dúvidas, de que o implante de chip invade a privacidade e a intimidade[10] das pessoas que trabalham, porquanto sua localização geográfica e o monitoramento de seus dados pessoais e sensíveis estarão constantemente sob domínio do empregador/empresa e, sendo assim, a título de conclusão deste ensaio, resta fazer-se a seguinte pergunta: a legislação pátria e os respectivos órgãos públicos de fiscalização são meios hábeis e eficazes de controle de quem possui o total domínio e manuseio dos dados das pessoas que trabalham?

Antes de responder esta pergunta convém não perder de vista que o contexto atual envolto em colapsos político-econômicos agravados por uma crise sócio-sanitária desencadeada pelo Corona Vírus, conjunturas atravessadas, ademais, por reformas trabalhistas e previdenciárias que retiraram de seu âmago um rol significativo de direitos sociais fundamentais consagrados, configuram uma flagrante ruptura do equilíbrio na constituição das relações de trabalho – motivo pelo qual, inclusive, gestaram-se o Direito do Trabalho e o Direito Previdenciário.

No que diz respeito ao objeto de análise deste ensaio, não há dúvidas de que todo este cenário de inovações tecnológicas e de comunicação refletiram e seguirão produzindo efeitos sobre os direitos das(os) trabalhadoras(es). Mas esta é apenas mais uma peça de um complexo quebra-cabeça que tem moldado as relações de trabalho contemporâneas, cujo panorama aponta, claramente, para a deterioração da função protetora do Direito do Trabalho tão indispensável nas sociedades digitais, tragadas pelo aumento do poder ilimitado das grandes empresas nacionais e transnacionais (BRANCO; TALPAI, 2020) e pela voracidade gananciosa de governantes desgovernados.

[10] Sobre o Direito a intimidade recomenda-se a leitura de PÉREZ LUÑO (2004).

REFERÊNCIAS BIBLIOGRÁFICAS

ARUFE VARELA, Alberto. Nuevas tecnologias, poder disciplinario y control del empresário. **Anuario de la Facultad de Derecho de la Universidad de la Coruña**, n. 8, 2004, La Coruña, p. 77-84.

ARTHURS, Harry. Who's afraid of globalization? Reflections on the future of labour law. In: Craig, John; Lynk, Michael (Ed.), **Globalization and the future of Labour Law**. Cambridge: Cambridge University Press, 2006.

BRANCO, Pedro Gonet; TALPAI, Bruno. A soberania e o ciberespaço: uma análise crítica do conceito de soberania e glozablização. **JURIS - Revista Da Faculdade de Direito** (Universidade Federal do Rio Grande – FURG), v. 30, n. 1, 2000, Rio Grande, p. 43–62.

CASTELLS, Manuel. **La era de la información**. Tradução de Carmen Martínez Gimeno e Jesús Alborés. 4.reimp. La sociedad en Red. Madrid: Alianza Editorial, 2000. v.1.

CASTELLS, Manuel; CARDOSO, Gustavo (ed.). **The Network Society: From Knowledge to Policy**. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2006.

COLÀS-NEILA, Eusebi. La Amenaza de los Derechos del Trabajador Derivada de la Innovación Tecnológica en la Empresa. **Creatividad y Sociedad**, n. 26, 2016, Madrid, p.263.

CRUZ VILLALÓN, Jesús. Poder de Dirección y Nuevas Estructuras empresariales. **Relaciones Laborales: Revista crítica de teoría y práctica**, n. 2, 2005, Madrid, p. 323-352.

ESCUDERO RODRÍGUEZ, Ricardo (Coord.). **El Poder de Dirección del Empresario. Nuevas Perspectivas**. Madrid: La Ley, 2005.

GOLDSMITH, Jack; WU, Tim. **Who controls the Internet? Illusions of a borderless world**. Oxford: Oxford University Pres, 2006.

PÉREZ DEL PRADO, Daniel. Instrumentos GPS y Poder de Control del Empresario. **Revista de Contratación Electrónica**, n. 107, 2009, Madrid, p. 49-73.

PÉREZ LUÑO, Antonio Enrique. El derecho a la intimidad. In: BETEGÓN CARRILLO, Jerónimo; LAPORTA, Francisco Javier; PRIETO SANCHÍS, Luis; RAMÓN DE PÁRAMO, Juan (Coord.), **Constitución y derechos fundamentales**. Madrid: Presidencia del Gobierno, Secretaría General Técnica, 2004, p. 639-668.

POLICY DEPARTMENT A; EP. **The Use of Chip Implants for Workers**.

Bruxelas: Directorate General for Internal Policies. Policy Department A: Economic and Scientific Policy/European Parliament (EP), 2018.

TEZANOS TORTAJADA, José Félix. Desigualdad y exclusión en las sociedades tecnológica. **Revista del Ministerio de Trabajo e Inmigración**, n. 35, 2002, Madrid, p. 35-54.

MORATO GARCÍA, Rosa María. **Derecho de Resistencia y Ejercicio Irregular del Poder de Dirección**. Granada: Editorial Comares, 2011.

ROTTER, Paweł; DASKALA, Barbara; COMPAÑÓ, Ramón. RFID implants: Opportunities and challenges for identifying people. **Technology and Society Magazine** (IEEE), v. 27, n. 2, 2008, Piscataway (New Jersey), p.24-32.

SÁNCHEZ-RODAS, Cristina Navarro. Poderes Directivos y Nuevas Tecnologías. **Relaciones Laborales: Revista crítica de teoría y práctica**, n. 138, 2017, Madrid, p. 163-184.

STOLZ, Sheila. Fim do trabalho ou trabalho sem fim? A terceirização laboral e a necessidade de dotar a legislação trabalhista internacional e local de uma "grande angular" protetivo regulatória, conditio *sine qua non* de justiça social. In: JUNIOR, Marco Aurélio et all. **Terceirização**: conceito, crítica, reflexos trabalhistas e previdenciários. São Paulo: LTr, 2018, p. 51-67.

_____. Os atores sociais e a concretização sustentável do direito fundamental ao trabalho garantido pela Constituição cidadã. In: **Direitos fundamentais e democracia I**. Coleção Conpedi/Unicuritiba.1 ed. Curitiba: Clássica Editora, 2014, v. 23, p. 488-551.

WILDER-SMITH, Annelies; FREEDMAN, David O. Isolation, quarantine, social distancing and community containment: pivotal role for old-style public health measures in the novel coronavirus (2019-nCoV) outbreak. **Journal of Travel Medicine**, v. 13, n. 27, mar, 2020, Oxford (U.K.), p. 1-4.