Editora Uniesp

DIREITO DIGITAL:

Tecnologias e Aplicações Emergentes

ORGANIZADORES:
José Carlos F. da Luz
Marcel Silva Luz
Patrícia Cristina F. Moura

uniesp
Centro Universitário

ISBN: 978-65-5825-092-0

DIREITO DIGITAL: TECNOLOGIAS E APLICAÇÕES EMERGENTES

José Carlos Ferreira da Luz
Marcel Silva Luz
Patrícia Cristina Ferreira Moura
(Organizadores)

Centro Universitário – UNIESP

Cabedelo - PB
2021

Designer Gráfico:
Mariana Morais de Oliveira Araújo

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Padre Joaquim Colaço Dourado (UNIESP)

L979d Direito digital: tecnologias e aplicações emergentes [recurso eletrônico] / Organizadores, José Carlos Ferreira da Luz, Marcel Silva Luz, Patrícia Cristina Ferreira Moura. - Cabedelo, PB : Editora UNIESP, 2021.
158 p. : il.

Tipo de Suporte: E-book
ISBN: 978-65-5825-092-0

1. Direito digital. 2. Inteligência artificial - Direito. 3. Tecnologia jurídica. 4. Responsabilidade civil - Internet. 5. Saúde digital - Direito. 6. Internet – Leis, legislação. 7. Direito - Tecnologia. I. Título. II. Luz, José Carlos Ferreira da. III. Luz, Marcel Silva. IV. Moura, Patrícia Cristina Ferreira.

CDU: 34:004

Bibliotecária: Elaine Cristina de Brito Moreira – CRB-15/053

Editora UNIESP

Rodovia BR 230, Km 14, s/n,
Bloco Central – 2 andar – COOPERE
Morada Nova – Cabedelo – Paraíba
CEP: 58109-303

SUMÁRIO

PREFÁCIO

A inteligência artificial está no centro da mudança histórica que estamos vivenciando. A robótica pode tornar possível um mundo melhor se ele estiver unido ao bem comum. Na verdade, se o progresso tecnológico aumenta as desigualdades, não é um verdadeiro progresso. Avanços futuros devem ser orientados no sentido de respeitar a dignidade da pessoa e da Criação. Vamos rezar para que o progresso da robótica e da inteligência artificial possam sempre servir à humanidade ... poderíamos dizer, "seja humano".
Papa Francisco, Intenção de Oração de novembro, 5 de novembro de 2020

Decisões de política e negócios com amplo impacto social são cada vez mais fundamentadas em tecnologia baseada em aprendizado de máquina, hoje comumente referida como inteligência artificial (IA). Ao mesmo tempo, a tecnologia de IA está se tornando cada vez mais complexa e difícil de entender, tornando mais árduo o controle quando não é usado de acordo com as leis existentes. Dadas essas circunstâncias, até mesmo os entusiastas da tecnologia exigem uma regulamentação mais rígida da IA. Os reguladores também estão intervindo e começaram a aprovar as respectivas leis, incluindo o direito de estar sujeito a uma revisão de decisões tomadas baseada exclusivamente no processamento automatizado no Artigo 20 da Lei Geral de Proteção de Dados (LGPD),

Como a digitalização se tornou uma tendência fundamental para transformar a economia em uma economia digital, as legislações são cada vez mais confrontadas com a tarefa de fornecer um quadro jurídico que permita colher crescimento econômico da digitalização. A atenção tem sido dada principalmente ao direito contratual, os desafios obviamente vão além dessa área do direito. Isso se torna particularmente claro com relação à IA. Sendo um impulsionador fundamental na construção de uma economia digital, a IA não só é um fator importante para colher o crescimento econômico, mas também traz riscos que precisam ser enfrentados.

Embora a crença de que algo precisa ser feito sobre IA seja amplamente compartilhada, há muito menos clareza sobre o que exatamente pode ou deve ser feito e como uma regulamentação eficaz pode parecer. Além disso, a discussão sobre a regulamentação da IA às vezes se concentra apenas nos piores cenários,

com base em casos específicos de mau funcionamento técnico ou mau uso humano de sistemas baseados em IA. Regulamentos com base em estratégias bem pensadas e esforço para equilibrar oportunidades e riscos de tecnologias de IA ainda estão faltando.

Este livro analisa os desafios factuais e jurídicos que a implantação da IA apresenta para os indivíduos e para a sociedade. As contribuições desenvolvem recomendações regulatórias que não restringem o potencial da tecnologia enquanto preservam responsabilização, legitimidade e transparência de seu uso. As análises e proposições são baseadas em normas, ou seja, considerar e desenvolver regimes estatutários e constitucionais que moldam ou restringem o projeto e o uso de IA. É importante ter em mente que a IA e as novas tecnologias fornecem instrumentos que abordam problemas da vida real que até agora os humanos tiveram que resolver: oficiais, médicos, motoristas, etc. Portanto, não basta perguntar se a IA 'funciona bem' ou 'é perigosa'. Em vez disso, é necessário comparar as características da nova tecnologia com as ações humanas correspondentes que ela substitui ou complementa, caso a caso.

Marcel Silva Luz

INTELIGÊNCIA ARTIFICIAL E TECNOLOGIA JURÍDICA: DESAFIOS AO ESTADO DE DIREITO

Marcel Silva Luz[1]
José Carlos Ferreira da Luz[2]

1 INTRODUÇÃO

A IA está moldando nossas vidas sociais. E também está afetando profundamente o processo de elaboração e aplicação da lei - cunhado pelo termo "tecnologia legal" ou "legal tech". Consequentemente, a lei como a conhecemos está prestes a mudar. Princípios básicos da lei, como responsabilidade, justiça, não discriminação, autonomia, devido processo legal e, acima de tudo, o estado de direito, estão em risco. Essas preocupações estão intimamente ligadas a uma "barreira da linguagem": tradicionalmente, "a lei precisa da linguagem como um peixe precisa de água". Mas os algoritmos seguem uma lógica diferente da linguagem humana. Apesar - ou talvez por causa - desses desafios, pouco foi dito sobre a regulamentação da tecnologia jurídica até agora, para a qual há obviamente uma demanda considerável. A questão não é se a tecnologia legal deve ser regulamentada, mas se a estrutura legal existente precisa ser ajustada ou refinada. Os legisladores hoje têm uma responsabilidade enorme; eles moldam as condições regulatórias iniciais. Essas decisões são cruciais, porque criarão novos caminhos. De acordo com Lawrence Lessing, devemos “construir, arquitetar ou codificar o ciberespaço para proteger valores que acreditamos serem fundamentais” (Lessing, 2006).

Neste artigo, sugere-se que reinventemos o estado de direito e o enxertemos com infraestruturas tecnológicas ao “desenvolver os padrões certos”, “definir os padrões certos” e traduzir os princípios jurídicos fundamentais em hardware e software. Em suma, “proteção legal desde o projeto” está em demanda com o objetivo de salvaguardar nossa capacidade humana de desafiar sistemas de decisão automatizados, fornecendo tempo e espaço para testar e contestar o

[1] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).
[2] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).

funcionamento de tais sistemas. E sua implementação deve ser exigida por lei — atribuindo responsabilidade quando necessário. Em última análise, isso reconciliará a tecnologia jurídica com o estado de direito. A hipótese inicial afirma que a lei permanece relevante, desde que os algoritmos não garantam a proteção efetiva das minorias e o bem comum. No entanto, a lei deve se reinventar sob a influência crescente da digitalização: deve se familiarizar com a lógica de um mundo digital. Soluções jurídicas podem ser encontradas apenas em cooperação com diferentes disciplinas acadêmicas, em particular, tecnologia e sociologia. Só então a lei acompanhará o mundo digital.

Este artigo está estruturado da seguinte forma: Na parte dois, será fornecida uma visão geral da tecnologia jurídica no uso público e privado. Na parte três, diferenças conceituais entre “lei” e “código” serão explicadas a fim de ilustrar por que a regulamentação é necessária. Na quarta parte deste artigo, será traçado o arcabouço constitucional e, na quinta parte, serão feitas as propostas de regulamentação da tecnologia jurídica. Os objetivos deste artigo são três: em primeiro lugar, fornecer uma visão geral da tecnologia jurídica no uso público e privado, em segundo lugar, examinar os desafios jurídicos levantados pelo desenvolvimento tecnológico recente. Em terceiro lugar, desenvolver diretrizes para a futura regulamentação legal de tecnologia, com foco na esfera jurídica europeia e anglo-americana. As propostas são baseadas na ideia de "proteção legal desde o projeto", com o objetivo de alinhar a tecnologia jurídica com o Estado de Direito.

2 CAMPOS DE APLICAÇÃO

Em um sentido amplo, a tecnologia jurídica cobre toda a tecnologia da informação usada no campo jurídico - e está inexoravelmente ligada aos dados. Tecnologia legal é um termo abrangente para qualquer tecnologia baseada em algoritmo em questões jurídicas - incluindo o uso público e privado. Para criar uma compreensão básica dos principais princípios operacionais da tecnologia legal, algumas definições e categorizações adicionais serão fornecidas.

2.1 DEFINIÇÕES

Um “algoritmo” é um processo ou conjunto de regras que definem uma sequência de operações a serem seguidas para resolver um determinado problema. Começando com uma “entrada”; as instruções descrevem um cálculo que, quando executado, prossegue através de um número finito de estados sucessivos bem definidos, eventualmente produzindo uma “saída”. Em outras palavras, um algoritmo é uma etapa de procedimento passo a passo para realizar uma tarefa ou função específica. “Código” é a implementação concreta do respectivo algoritmo.

Com base nessas definições, o escopo de possíveis aplicações de tecnologia legal é enorme. Em particular, com o surgimento de "Big data" e "IA", mudanças disruptivas surgiram no cenário jurídico. “Big data”, por um lado, é definido como “[...] ativos de informação de alto volume, alta velocidade e alta variedade que exigem formas inovadoras e econômicas de processamento de informações para melhor percepção e tomada de decisão” (GARTNER, 2021).

Foi corretamente observado que estamos vivendo em uma época de entusiasmo movido a dados, dados, por exemplo, os investimentos que são feitos por governos, universidades e entidades privadas para coletar e armazenar dados e extrair novos conhecimentos desses bancos de dados em constante crescimento. IA por outro lado refere-se à análise de dados para modelar algum aspecto do mundo. As inferências desses modelos são então usadas para prever e antecipar possíveis eventos futuros. A IA permite que as máquinas aprendam com a experiência, progredindo constantemente para imitar as habilidades cognitivas humanas. Em última análise, trata-se de "dar aos computadores comportamentos que seriam considerados inteligentes em seres humanos" (MEDINA, 2015).

Uma das abordagens de IA de crescimento mais rápido é o "aprendizado de máquina". Este conjunto de técnicas e ferramentas permite que os computadores "pensem" e resolvam problemas "de forma independente e eficiente". Por definição, "aprendizado de máquina é um subconjunto da IA - uma aplicação poderosa da tecnologia de IA", em que as máquinas são expostas a grandes conjuntos de dados e fornecido com mecanismos para aprender de forma independente e se tornar cada vez mais “inteligente”.

Para encontrar um acesso analítico à tecnologia jurídica, é essencial dividir o conceito em diferentes categorias. Para fins regulatórios, uma primeira distinção é feita entre o uso público e privado de tecnologia legal. Há uma diferença, por exemplo, entre a maneira como a tecnologia jurídica é aplicada por uma firma de direito privado e a maneira como é aplicada pela polícia. Enquanto as entidades privadas são movidas por motivos econômicos, as autoridades estatais devem servir ao interesse público. Para fins regulatórios, essa diferenciação é altamente relevante. Uma segunda diferenciação diz respeito à aplicação de tecnologia jurídica como uma "ferramenta de previsão investigativa" usada em um processo de tomada de decisão para gerar novos conhecimentos, ou como um "substituto de decisão" (não requerendo nenhuma intervenção humana adicional). Essas duas diferenças são importantes quando se trata de regulamentar a tecnologia jurídica. Os diferentes padrões e justificativas aplicáveis serão desenvolvidos na quinta parte deste artigo. A seguir, uma visão geral do uso público e privado de tecnologia legal é fornecida, a qual, dada a rapidez dos desenvolvimentos tecnológicos, obviamente reflete apenas o momento atual.

2.3 O USO PÚBLICO DE TECNOLOGIA LEGAL: STATUS QUO E TENDÊNCIAS

No que diz respeito ao uso público de tecnologia legal, a aplicação da lei assumiu um papel pioneiro nos países mais desenvolvidos. Em vários países europeus, a polícia implementou o uso de novas tecnologias quem visa ajudá-los a prever crimes futuros antes que se materializem - uma iniciativa chamada "policiamento preditivo".

O policiamento preditivo não apareceu do nada. Em vez disso, está firmemente ancorado em uma longa linhagem de estratégias de policiamento, que por sua vez foram impactadas por avanços tecnológicos e programas políticos. Para compreender formas específicas de policiamento preditivo e seus efeitos no trabalho policial, é importante situar as trajetórias históricas mais amplas de como a polícia produz conhecimento e previne o crime. Na verdade, há pouco consenso sobre se e, em caso afirmativo, como o policiamento preditivo pode ser claramente diferenciado de formas anteriores de análise de crime, mapeamento de crime e outras formas de gerenciamento, planejamento e ação com suporte de computador. O policiamento

preditivo deve ser colocado dentro de várias tendências globais no policiamento: digitalização, cientificação, a mudança para a ação orientada para o futuro, pressão econômica e política sobre as organizações policiais, bem como as estratégias de policiamento, técnicas de patrulhamento e programas de prevenção ao crime que têm surgiram dessas tendências (MCDANIEL AND PEASE, 2021).

Além disso, o policiamento preditivo não é um fenômeno único. Pode-se defini-lo como o uso proativo de análise de dados mediada por algoritmos com o propósito de encontrar padrões em conjuntos de dados, com base nos quais estimativas de risco são produzidas para indivíduos ou locais e são operacionalizadas na forma de medidas de prevenção direcionadas. No entanto, não é um modelo, não é um processo, não é um algoritmo e não é um aplicativo de software (MCDANIEL AND PEASE, 2021).

Em vez disso, na última década, “policiamento preditivo” surgiu como um termo coletivo para uma infinidade de maneiras pelas quais a polícia busca lidar com o futuro usando a análise algorítmica de dados para modulá-lo. Pode ser baseado em conjuntos estreitos de dados criminais produzidos pela própria polícia ou pode integrar fontes de dados heterogêneas. Ele pode ser originado em algoritmos estáticos e apoiado em regras ou pode incorporar a dinâmica do aprendizado de máquina.

Pode ser usado para prever o crime em locais específicos ou para prever o crime de pessoas específicas. Ele pode integrar informações ambientais dinâmicas, como dados meteorológicos ou de tráfego. Pode ter como alvo roubo, furto de carro, furto de carteira ou violência de gangues. Pode ser desenvolvido e projetado pela polícia ou por empresas privadas. E esses são apenas alguns dos recursos possíveis que explicam as variações entre as diferentes abordagens. Portanto, é preciso definir cuidadosamente do que estamos falando quando nos referimos ao policiamento preditivo.

Na Inglaterra, o policiamento preditivo foi recentemente apoiado pelo Supremo Tribunal e a polícia alemã também introduziu essa nova tecnologia. O sistema de “previsão de crimes” exibe os níveis de risco para diferentes áreas e os aplica a mapas de calor. Os policiais podem estar no local antes que ocorra o próximo crime. Os defensores das ferramentas técnicas argumentam que esses tipos de análises são mais precisos e menos tendenciosos do que os resultados que

os humanos podem fornecer e, em última análise, tornam mais fácil focar no policiamento preventivo e prevenção (RADEMACHER, 2017).

É claro que a aplicação de tecnologia jurídica na administração pública não se limita ao policiamento preditivo. Ele se estende a muitos campos: a saber, aplicativos de IA são usados na gestão administrativa do tráfego rodoviário. Em particular, os sistemas de controle de tráfego inteligente em rodovias coletam vários dados por meio de sensores e regulam o tráfego de acordo, por exemplo, indicando proibições de ultrapassagem ou limites de velocidade. Com base nos dados coletados, atos administrativos automatizados são emitidos. Da mesma forma, a IA é usada em processos tributários. Na Alemanha, por exemplo, a identificação de risco impulsionada por IA já se tornou, ao que parece, parte dos sistemas regulares de gestão tributária, que decidem quem deve apresentar seus documentos comprovativos para auditorias fiscais (DRESSEL AND FARID, 2018).

Mesmo no judiciário, a tecnologia legal já está sendo usada. O procedimento automatizado de cobrança de dívidas é um primeiro exemplo simples na Alemanha. Não é novidade que os Estados Unidos estão muito mais à frente nesse aspecto, usando software que se tornará a base para a tomada de decisões em um processo judicial posterior. COMPAS (Perfil de Gestão de Criminosos Correcional para Sanções Alternativas), por exemplo, foi implementado em vários estados dos EUA e também foi introduzido em 2012 pelo Departamento de Correções (DOC) em Wisconsin. O sistema visa prever com segurança o risco de reincidência criminal. Para cada infrator, o COMPAS calcula uma "pontuação de risco" individual que terá um impacto na sentença subsequente. A lógica subjacente é simples: se o software pontua um alto risco para um réu em uma escala de 1 a 10, o juiz não permite liberdade condicional, mas impõe uma sentença de prisão (PASQUALE, 2017).

Embora este software tenha sido altamente criticado por alguns, que rejeitam a ideia de um algoritmo que ajude a mandar uma pessoa para a prisão, outros elogiam o COMPAS como uma ferramenta confiável de aprendizado de máquina. Outros estudos foram iniciados pelos proponentes para fornecer uma prova convincente dos benefícios: com base em conjuntos de dados de cerca de 150.000 casos de crimes nos EUA, uma simulação de política mostra que uma regra de liberação de acordo com as previsões de aprendizado de máquina reduziria a população carcerária em 42%, sem aumento nas taxas de crime, ou reduziria as

taxas de criminalidade em 25% sem alterar a população carcerária (KLEINBERG et al. 2017).

O que devemos pensar nessas promessas? Podemos confiar na IA para decidir imparcialmente - sem ter uma visão do funcionamento interno de um sistema como o COMPAS? Como os juízes e júris podem usar as evidências produzidas pela IA? E até que ponto os tribunais devem confiar na IA como uma ferramenta para regular o comportamento quando se trata de decisões cruciais, como sentenças criminais? O que está em jogo quando as aplicações de IA falharam? As respostas críticas serão fornecidas abaixo.

Esses exemplos mostram que o cenário jurídico mudará drasticamente à medida que a IA progrida continuamente para imitar as habilidades cognitivas humanas. A tecnologia jurídica não é mais apenas para digitalizar o ambiente de trabalho e fornecer ferramentas individuais de aprimoramento da eficiência, mas para permitir que as máquinas assumam o núcleo atividades legais na esfera privada e a pública (SUSSKIND 2013).

A questão, portanto, que surge é se o “ciber-tribunal” e o “advogado robô” não são mais apenas ficção científica, mas uma imagem realista do que o futuro pode trazer. A resposta é não, provavelmente não. Partes interessadas de diferentes áreas - que vão desde autoridades governamentais, acadêmicos a corporações - rejeitaram a ideia de que a IA atingiu “capacidades sobre-humanas totalmente autônomas”, pelo menos até agora. No entanto, o desenvolvimento tecnológico continua e a tecnologia legal será um desafio cada vez maior para a lei nos próximos anos (WAGNER, 2018).

Hoje, a indústria de tecnologia jurídica cresceu em todo o mundo. Elas desenvolvem aplicativos de TI que visam dominar tarefas cada vez mais complexas. Essas aplicações promissoras caem em terreno fértil. A tecnologia jurídica não apenas fornece respostas à crescente eficiência e às pressões de custo no setor jurídico, mas também pode ajudar a melhorar o acesso à justiça - pelo menos potencialmente. No entanto, é uma questão bem diferente se a tecnologia jurídica será capaz de lidar com problemas regulatórios complicados que requerem consideração cuidadosa. Nesse ponto, o ceticismo é justificado (WAGNER, 2018). Os problemas que podem ocorrer serão examinados a seguir.

3 DIFERENÇAS CONCEITUAIS ENTRE “LEI” E “CÓDIGO” (digital)

Foi mencionado que as diferenças na "lei" e no "código" exigem conceitos regulamentares diferentes. Nesta seção, os princípios operacionais de “lei” e “código” serão justapostos, a fim de detectar problemas e necessidades regulatórias. Aspectos técnicos e dogmáticos devem ser considerados igualmente. A atenção também será chamada para a questão sociológica sobre o que realmente significa estabelecer e aplicar a lei.

3.1 APLICAÇÃO DA LEI COMO UM ATO SOCIAL

Em primeiro lugar, deve-se chamar a atenção para o fato aparentemente trivial de que as normas jurídicas (escritas) são “trabalho humano” e “atos sociais” - assim como a aplicação e interpretação da lei em cada caso individual. Aplicação de uma norma jurídica é um processo exigente: primeiro, é necessária uma etapa de concretização, porque as normas jurídicas geralmente são redigidas em termos gerais. Esse processo costuma ser mais desafiador quanto mais abstrata for uma disposição. Considere, por exemplo, o princípio de "boa fé" codificado nos artigos 113 e 422 do Código Civil Brasileiro. Após a concretização, a norma pode ser aplicada a um caso particular.

É fundamental perceber que o direito só pode existir "na linguagem e por meio da linguagem", o que traz consigo uma abertura à interpretação. No entanto, o ato de interpretação legal não é uma "operação mecânica direta de análise textual" é muito mais complexo e requer conhecimentos complementares, especialmente onde há margem para discricionariedade. Tomemos, por exemplo, o campo da prevenção de riscos jurídicos, que depende de conhecimentos técnicos.

As implicações na vida real de uma disposição legal devem ser consideradas seriamente: se a lei deve servir como um instrumento de controle comportamental, o advogado deve estar atento não apenas aos efeitos imediatos, mas também aos longos, tais como as consequências sociais a longo prazo. Em outras palavras, os profissionais do direito e os legisladores não devem fechar os olhos para as consequências da lei. Para concluir, a aplicação da lei é um ato

independente de "produção legal". Em cada caso individual, a lei é recriada como um "produto social".

3.2 CÓDIGO COMO UM ATO TÉCNICO

Como as suposições básicas sobre a aplicação da lei mudam quando os computadores substituírem advogados? Claro, algoritmos são feitos por humanos; são "atos sociais" em primeiro lugar.51 Este fato aparentemente óbvio tem consequências de longo alcance. Melvin Kranzberg vai direto ao ponto ao afirmar: “As tecnologias não são boas nem más, nem neutras.” Além disso, “lei” e “código” diferem significativamente em sua aplicação (KRANZBERG, 1986).

Os algoritmos não são escritos em uma linguagem natural, mas em uma linguagem técnica: um código binário mapeia informações através das sequências dos dois sistemas de símbolos “1” e “0”. Assim, a codificação de um software de tecnologia jurídica consiste em dois desafios-chave de tradução. Em primeiro lugar, a "lei" deve ser convertida em código binário e, em segundo lugar, deve ser traduzida de volta para a linguagem natural. Impulsionados por essa lógica, os algoritmos traduzem a realidade social em código binário: extraídos de inferências aleatórias, no entanto, eles podem apenas identificar correlações, não causalidades (WISCHMEYER, 2018).

Todo software baseado em IA é limitado a essa lógica binária. No entanto, formas avançadas de sistemas baseados em IA - os chamados sistemas de aprendizagem - são capazes de transformar novos dados (input) em decisões (saída) sem intervenção humana significativa. “Sistemas responsivos” podem até mesmo modificar dinamicamente os padrões de decisão anteriores. Assim, o processo de tomada de decisão é condicionado pelas experiências de aprendizagem de um sistema dirigido por IA. Isso, por sua vez, pode levar a decisões estruturalmente imprevisíveis. No entanto, o impossível permanece impossível: os algoritmos não têm "bom senso" e fatores de decisão "leves", como intuição, julgamento de valor ou pensamento holístico (WISCHMEYER, 2018).

3.3 EQUÍVOCOS DE “CÓDIGO”

Conforme já indicado, a tecnologia jurídica se baseia na noção de que as normas jurídicas podem ser formalizadas e totalmente traduzidas para a linguagem de computador. Para verificar esta afirmação, devem-se revelar os diferentes princípios operacionais de “lei” e “código”. Tradicionalmente, a aplicação da lei não é percebida como um processo estritamente formalizado, especialmente com o aumento do poder discricionário de advogados e juízes. Um advogado ou juiz não aplica a lei no sentido matemático-formal, mas sim no sentido dialético.

O processo de aplicação e interpretação de uma norma jurídica requer julgamentos de valor, conhecimento intuitivo e pensamento holístico. No entanto, os algoritmos carecem de qualquer uma dessas qualidades humanas e há poucas perspectivas de que os programadores de software sejam capazes de preencher essa lacuna. Embora as máquinas possam, em um futuro próximo, executar algumas das tarefas legais repetitivas, estamos longe de substituir as nuances que valorizam o julgamento e a experiência e talvez nunca o façamos (Pfeifer, 2018).

Surge outra questão crítica: a linguagem natural pode ser transformada na linguagem binária de um sistema de computador? Embora a linguagem natural tenha certa lógica inerente devido à sua gramática, o significado de uma palavra pode variar significativamente dependendo do contexto.

As distinções linguísticas não são inteiramente previsíveis ou programáveis. Apenas em casos simples e diretos é a formalização imaginável (no entanto, é difícil determinar previamente se um caso é fácil ou complexo), mas em uma situação legal ou factual difícil, a formalização falha. Em conclusão, é bastante óbvio que a formalização da linguagem jurídica não é nem semanticamente possível nem desejável. No entanto, a lei precisa ser flexível para lidar com fenômenos técnicos ou sociais complexos no melhor interesse da sociedade. O grau necessário de flexibilidade é fornecido pela linguagem humana (LA DIEGA, 2018). Nesse ponto, uma diferença categorial entre "lei" e "código" se torna manifesta exigindo novas formas de regulamentação.

Por que a regulamentação legal é necessária no mundo digital? A resposta é simples. A função social do direito é, acima de tudo, servir o bem comum e a proteção das minorias. Mas nenhuma das categorias importa no "código" digital.

Enquanto essa situação persistir, o direito público continuará sendo um instrumento indispensável de controle e regulação. Em outras palavras: a atuação do estado é importante, pois, como já ilustrado, os computadores não compreendem as normas sociais e a linguagem.

A forma como os legisladores podem preencher essas lacunas e as situações em que ocorrem conflitos com os princípios constitucionais básicos serão analisadas na seção seguinte.

4 MARCO CONSTITUCIONAL

Esta seção irá delinear as diretrizes constitucionais para o desenvolvimento e aplicação de software de tecnologia legal. Como uma primeira etapa, esta seção examinará por que a tecnologia jurídica pode representar um risco para o estado de direito e a democracia. Numa segunda etapa, serão destacados os potenciais conflitos entre a tecnologia jurídica e o direito à privacidade. Finalmente, esta seção analisará por que a tecnologia jurídica pode entrar em conflito com o direito a não discriminação.

4.1 ESTADO DE DIREITO E DEMOCRACIA

Em primeiro lugar, as críticas sérias à tecnologia legal dizem respeito às condições (legais) sob as quais o software é desenvolvido. Este processo ocorre muito além do controle do estado. Foi corretamente criticado que o desenvolvimento de software, mesmo de código aberto, não é transparente sendo concentrado em uma pequena comunidade de programação, muitos dos quais são empregados por poucas empresas oligopolistas diretamente responsáveis e sem nenhum controle externo. Este procedimento não oferece nenhuma possibilidade para as pessoas potencialmente afetadas intervirem ou mesmo participarem (O'HARA, 2017).

Os desenvolvedores de software até desfrutam da proteção de segredos comerciais e não precisam revelar seus algoritmos. A falta de controle resultante pode ter consequências sérias: embora os desenvolvedores de software estejam certamente dispostos a serem neutros e objetivos, eles nunca podem escapar

totalmente do preconceito, costumes, cultura, conhecimento e contexto ao desenvolver algoritmos (LA DIEGA, 2018).

A maioria dos algoritmos é deliberadamente criada para propósitos que estão longe de ser neutros: gerar receita, estimular comportamentos e estruturar preferências de certa maneira, para identificar e classificar pessoas. Nessa perspectiva, o programador de computador é um criador de universos dos quais somente ele é o legislador. Colocado de outra forma, os desenvolvedores de software se tornarão "quase legisladores" sem responsabilidade ou controle externo, se os legisladores não conseguirem moldar as condições regulatórias no melhor interesse da sociedade.

Dessa forma, o desenvolvimento de software - especialmente na falta de transparência - desencadeia uma série de preocupações sobre o estado de direito. Neste contexto, o estado de direito deve ser interpretado numa perspectiva mais ampla de que as pessoas devem obedecer às leis e serem reguladas por elas, porém, em uma teoria política e jurídica, ele deve ser lido de uma maneira mais estrita, no sentido de que o governo deve ser regulado pelas leis e submetido às mesmas (VIEIRA, 2021). Um elemento crucial é o direito de contestar a aplicação e a validade de uma norma legal, normalmente perante um tribunal. Em resumo, no estado de direito são indissociáveis a responsabilidade, justiça e o devido processo legal.

Ao passar do desenvolvimento de software para a aplicação de software de tecnologia legal, a situação é ainda mais crítica: o estado de direito está exposto a sérios riscos potenciais, especialmente quando a tecnologia legal for aplicada por autoridades estatais que devem servir o interesse público. Enquanto o funcionamento interno das tecnologias de IA estiver protegido da visão do público, as pessoas não poderão contestar qualquer suspeita de violação ou manipulação de seus direitos. Esta “desumanização da tomada de decisão” coloca em questão o devido processo legal, e a capacidade de apelar de forma significativa de uma decisão adversa (VIEIRA, 2021). Outra objeção diz respeito à diferenciação acima mencionada entre a tecnologia legal usada como uma “ferramenta de previsão investigativa” no processo de tomada de decisão de um juiz ou como um “substituto de decisão” em substituição a decisão de um juiz (ver subitem 2.3).

A decisão pode ter consequências graves: se os juízes gradualmente trocarem o raciocínio verbal ordinário por métodos baseados em IA, eles minam a complexidade de um julgamento. O princípio do devido processo legal concede aos réus o direito de entender do que são acusados e quais são as provas contra eles. Esse direito, entretanto, está em jogo quando os tribunais ou outras autoridades estatais (parcial ou mesmo totalmente) baseiam suas sentenças apenas em algoritmos secretos. Embora possa ser útil que os juízes confiem em algoritmos "para melhorar a qualidade e a consistência de suas decisões, eles não devem permitir que os algoritmos decidam em seu lugar" (LA DIEGA, 2018).

Como indicado acima, os algoritmos "carecem de uma bússola ética". As questões surgem, portanto, até que ponto o governo deve garantir que o estado de direito e a participação democrática se tornem características de qualidade de um "bom" algoritmo (MARTINI, 2017). Mas quanta intervenção governamental é apropriada? Os legisladores se deparam com um intrincado ato de equilíbrio: os desenvolvedores de software privados ou estatais devem divulgar seu código-fonte para inspeção pública ou devem estar sujeitos a algum tipo de controle? Uma tarefa desafiadora! As respostas serão desenvolvidas na quinta parte deste artigo.

4.2 DIREITO À PRIVACIDADE

Como já indicado, a tecnologia legal pode acarretar sérios riscos para o direito à privacidade - tanto em uso público como privado. Sem qualquer percepção do funcionamento interno do software de tecnologia legal, as pessoas têm pouco controle sobre como os respectivos aplicativos coletam e armazenam seus dados pessoais. A situação se tornou ainda mais precária com o surgimento da análise baseada em dados.

O que se quer dizer quando se fala em "privacidade" e onde estão os limites constitucionais para tecnologia? De acordo com uma noção comum, o direito à privacidade diz respeito à escolha, autonomia e liberdade individual. Inclui o direito de determinar o que uma pessoa em particular manterá oculto e o que, como, quando e para quem essa pessoa divulgará informações pessoais. Os termos “privacidade”, “privacidade de informação”, “privacidade de dados” e “proteção de dados” são frequentemente usados como sinônimos, a fim de enfatizar o direito de

controlar a coleta e o processamento de dados pessoais por governos e entidades privadas.

No Brasil, a Constituição Federal no art. 5º, inciso XII estabelece que "é inviolável o sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" e o inciso X do art. 5º da Constituição garante: a inviolabilidade da intimidade e da vida privada, da honra e da imagem das pessoas.

Com base nesses requisitos constitucionais a LGPD estabeleceu expressamente no art. 2º, II, o direito à autodeterminação informativa - considerada como um direito fundamental moderno à proteção de dados - introduzindo padrões uniformes para o processamento de dados pessoais no Brasil.

Para cumprir as regras de proteção de dados, as empresas e outras organizações (estatais) devem seguir os princípios fundamentais de processamento de dados definidos no Artigo 6º da LGPD, nomeadamente transparência, limitação da finalidade, minimização de dados, exatidão, limitação de armazenamento, integridade e confidencialidade. Em particular, eles devem fornecer informações onde os dados pessoais são coletados do titular dos dados (Artigo 9º da LGPD) - uma disposição que é altamente relevante quando se trata de análise de big data. Além disso, a LGPD exige que operadores sejam transparentes e compreensíveis na comunicação com os usuários.

Além disso, eles são obrigados a responder às solicitações dos usuários de acesso aos seus dados, sua retificação ou apagamento (Artigos 15 a 17 da LGPD). Além disso, o Artigo 18, §2º da LGPD implica o direito de oposição, permitindo que indivíduos solicitem a uma empresa a interrupção do processamento de seus dados pessoais, porém o direito de objetar não é absoluto; como outros direitos civis, pode ser restringido quando conflitar com o interesse público.

Outra disposição particularmente importante quando se trata de tecnologia jurídica e análises de big data é o caput do Artigo 20 da LGPD - Tomada de decisão individual automatizada - que assegura ao titular dos dados tem o direito de revisão a uma decisão baseada exclusivamente em processamento automatizado:

> (...) a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil

> pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Ressalte-se ainda que o §2º do mesmo Artigo 20 prevê a possibilidade da autoridade nacional realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

4.3 DIREITO À NÃO-DISCRIMINAÇÃO

As objeções mencionadas contra a tecnologia legal - especialmente a falta de transparência - também podem acarretar efeitos colaterais negativos sobre o direito à não discriminação. Essas preocupações estão relacionadas ao fato de que o software baseado em algoritmo possivelmente aprofundará e acelerará os processos de selecionar e classificar as pessoas - sem qualquer possibilidade de controle para aqueles que são potencialmente afetados. A discriminação pode ser definida como qualquer tratamento injusto de um indivíduo por causa de sua filiação um grupo particular, por exemplo: raça, sexo, religião, entre outros. O direito a não discriminação está explicitamente previsto na Constituição Federal (CF, 3°, IV) quando estabelece o objetivo de promover o bem de todos, independentemente de origem, raça, cor, idade e toda e qualquer forma de discriminação e na Declaração Universal dos Direitos do Homem ao dispor que todos os seres humanos nascem livres e iguais em dignidade e em direitos (art. 1°); sendo iguais perante a lei, tendo direito à igual proteção legal contra qualquer discriminação que viole dispositivos da Declaração, bem como qualquer incitamento a esta prática (art. 7°).

Medido em relação a esses padrões, o uso de tecnologia legal pode, em certo sentido, ser considerado inerentemente discriminatório.

Um estudo descobriu que o software COMPAS (ver subitem 2.3) prevê que réus de cor da pele negra terão maiores riscos de reincidência do que realmente têm, enquanto réus brancos têm taxas mais baixas do que realmente fazem. Embora os dados usados pelo COMPAS não contenham a raça de uma pessoa, outros aspectos dos dados coletados podem ser correlacionados à raça que pode acarretar disparidades raciais nas previsões. Esses resultados mostram: o aprendizado de máquina depende de dados que foram coletados da sociedade e, na medida em que a sociedade contém desigualdade, exclusão ou discriminação, essas questões

sociais existirão nos dados. Ainda mais, o aprendizado de máquina pode perpetuar os padrões existentes de discriminação (DRESSEL AND FARID, 2018).

Na verdade, a tecnologia jurídica pode ser ainda "pior" do que advogados humanos - devido à falta de transparência e responsabilidade. Onde os conjuntos de dados são tidos como confiáveis sem qualquer revisão e controle humano adicional, o computador irá exacerbar os preconceitos. Qual é a raiz do problema? O princípio fundamental de não discriminação não é uma categoria relevante no “código”. Lembre-se do fato de que os algoritmos "carecem de uma bússola ética" (MARTINI, 2017). O que é necessário? Como Angwin corretamente afirma, IA e ciências jurídicas "têm que andar de mãos dadas para proteger o princípio da não discriminação contra novas formas de marginalização social no mundo digital" (ANGWIN et al. 2016).

5 PROPOSTAS DE “REGULAMENTAÇÃO POR PROJETO”: UMA LEI DE EQUILÍBRIO

Nesta seção, algumas reflexões serão apresentadas sobre como as regras regulatórias existentes podem ser alinhadas com os princípios constitucionais mencionados acima. Embora essa exploração não seja exaustiva, ela servirá como um convite à participação em pesquisas interdisciplinares e como uma diretriz para a futura regulamentação legal de tecnologia. A estratégia é dupla: primeiro, devemos garantir que as tecnologias de IA se desenvolvam de forma a garantir as normas sociais. Em segundo lugar, devemos encontrar maneiras de incorporar esses princípios à tecnologia.

5.1 REALINHAMENTO REGULATÓRIO

O que é importante do ponto de vista regulatório? As ferramentas regulatórias existentes devem ser complementadas com meios inovadores para fazer frente aos rápidos desenvolvimentos tecnológicos. Para este efeito, a abordagem tradicional de “comando e controle” deve ser rejeitada como inadequada. Em vez disso, a regulamentação legal deve redesenhar suas estruturas usuais de controle unilateral e determinista passando para a "comunicação". O que se quer dizer aqui é a “comunicação” entre advogados e desenvolvedores de software, a fim

de aprender com a disciplina uns dos outros - um esforço que tem sido associado à noção de "proteção legal desde o projeto".

5.2 PROTEÇÃO LEGAL DESDE O PROJETO COMO UM PONTO DE PARTIDA

Por muito tempo, os legisladores negligenciaram o poder do design, mas recentemente a frase "proteção legal desde o design" alcançou grande popularidade. De acordo com as descobertas sociológicas, o design é poderoso. Pode influenciar as normas e expectativas da sociedade. Com base nesse conhecimento, a lei deve orientar o projeto da tecnologia da informação para proteger os valores constitucionais (HARTZOG, 2018).

O que exatamente significa quando se fala em "proteção legal desde o projeto" ou "Privacy by Design"? O conceito foi desenvolvido nos anos 1990 e ganhou reconhecimento internacional desde então, sendo recepcionado pelo GDPR, artigo 25.º, n.º 1, "Proteção de dados desde a concepção e por defeito". De acordo com esta disposição o controlador deve, tanto no momento da determinação dos meios de processamento e no momento do próprio processamento, implementar medidas técnicas e organizacionais adequadas, tais como pseudonimização, que são concebidas para implementar princípios de proteção de dados, tais como minimização de dados, de forma eficaz e integrar as salvaguardas necessárias no processamento, a fim de proteger os direitos do titular dos dados (VENTURA, 2021).

A ideia do “Privacy by Design” também vem inserida na LGPD (Lei Geral de Proteção de Dados), e é uma grande aliada na adequação à legislação, pois configura uma boa prática nas operações de tratamento de dados pessoais.

A lógica por trás da "proteção de dados desde o projeto" é que a proteção de dados e os princípios de privacidade devem ser incorporados à tecnologia. Isso traz à tona o termo "design", que descreve "como um sistema é arquitetado, como funciona, como se comunica e como essa arquitetura, função e comunicação afetam as pessoas". O “bom design” não pode ser alcançado sem a participação e respeito de todas as partes interessadas, incluindo engenheiros, executivos, usuários e advogados. A proteção desde o projeto é uma abordagem proativa ex ante para considerar e proteger a privacidade e outras normas gerais no desenvolvimento de um grupo (por exemplo, negócios), ação (por exemplo, informação), ou coisa (por

exemplo, tecnologia). Muitas vezes, a (pior) alternativa é responder aos danos à privacidade (ex post) depois que eles ocorreram.

Com o conceito de "proteção desde o projeto", a comunicação entre advogados e desenvolvedores de software é necessária e gerenciável. Se os legisladores decidirem se preocupar com o design, eles não terão que reinventar a roda ou dominar a tarefa por conta própria. Existe uma disciplina de desenvolvimento de software robusta e bem estabelecida, dedicada ao design de proteção da privacidade. Os reguladores governamentais não devem ignorar a experiência "daqueles já comprometidos em alavancar o design tecnológico para proteger nossa privacidade" e valores sociais. Além disso, as lições aprendidas com o design a regulamentação em outros campos e jurisdições pode ser útil ao regulamentar a tecnologia legal.

Em poucas palavras, quais são os principais problemas? "Ignorar o design é perigoso, mas também o é a superregulação, e um equilíbrio importante deve ser alcançado." Como isso pode ser feito? No item seguinte, serão apresentados os principais elementos da "proteção legal desde o projeto". Em parte, as disposições existentes devem ser reformadas; em parte, eles devem ser completamente redefinidos e revisados. Desse modo, as distinções tipológicas e regulatórias entre o uso público e privado de tecnologia legal serão consideradas.

5.3 DIRETRIZES REGULATÓRIAS

Como foi demonstrada nas seções anteriores, a falta de transparência e controle pode impedir as pessoas de exercerem plenamente seus direitos (especialmente a privacidade e a não discriminação). No entanto, onde os direitos fundamentais são restringidos por tecnologia legal, uma justificação normativa é necessária; onde os funcionários públicos aplicam tecnologia jurídica, a transparência é um princípio fundamental do estado de direito. Até que ponto a lei atual já atende a esses requisitos e quais reformas são necessárias?

O caput do Artigo 20 da LGPD - Tomada de decisão individual automatizada - que assegura ao titular dos dados tem o direito de revisão a uma decisão baseada exclusivamente em processamento automatizado. A ideia por trás dessa disposição é "capacitação individual": As pessoas devem ser mantidas informadas e protegidas

da tomada de decisão automatizada sempre que possível. Portanto, de acordo com o Artigo 20, deve ser garantido que uma decisão automatizada é revisada por um ser humano.

Mas para que essa revisão não seja mera formalidade, como o é a maioria dos consentimentos, a revisão deve ser feita por alguém que tem autoridade e competência para mudar a decisão. Ainda assim, surge a questão, se e em que medida a revisão humana finalmente se desviará de uma decisão automatizada anterior. Na prática, é improvável que a supervisão humana vá realmente além de uma mera verificação de plausibilidade.

Em particular, as pessoas devem ser informadas sobre o processamento de dados baseado em IA, em um formato facilmente compreensível que lhes permita reagir a uma decisão de uma forma significativa.

Além disso, a fim de equilibrar as assimetrias de conhecimento (devido toa complexidade dos conjuntos de dados) mecanismos de controle coletivo devem ser implementados de modo que software com potencial impacto em dados confidenciais deve passar pelo controle do governo. Esta “verificação de algoritmo” deve cobrir não apenas o código do programa em si, mas também a qualidade e confiabilidade do programa de treinamento de software. Esta inspeção deve ser obrigatória para qualquer aplicação estatal de tecnologia com impacto potencial em dados confidenciais.

O controle governamental deve se estender à validade e à precisão do banco de dados. Algoritmos de controle podem ajudar a analisar sistematicamente os processos automatizados de tomada de decisão, especialmente para descobrir preconceitos e discriminação. Além disso, os desenvolvedores de software devem ser obrigados a estabelecer sistemas de gerenciamento de risco, a fim de garantir que os aplicativos de software não produzam decisões discriminatórias ou tendenciosas.

Eventualmente, cada sistema de tecnologia legal deve ser projetado para dar aos usuários e outros sujeitos do sistema a capacidade de avaliar a responsabilidade do sistema por meio de algoritmos e conjuntos de dados. Além disso, a transparência e a responsabilização devem ser garantidas para aqueles que são potencialmente afetados. Só então, as pessoas seriam capazes de contestar as consequências jurídicas de qualquer processo tecnológico.

Um bom design de tecnologia requer intensa cooperação entre especialistas técnicos e jurídicos garantindo que os valores constitucionais fundamentais possam ser embutidos em algoritmos. Aplicada corretamente, a tecnologia baseada em IA não apenas fará previsões mais precisas, mas fornecerá maior transparência e justiça em comparação com suas contrapartes humanas.

5.4 O “FATOR HUMANO”

Finalmente, alguns comentários devem ser feitos sobre a educação jurídica. Como foi demonstrado acima, “proteção legal desde o projeto” requer esforço interdisciplinar. A mudança tecnológica que os advogados testemunham traz em seu rastro a obrigação para os juristas de se familiarizarem com as oportunidades e consequências das ferramentas impulsionadas pela IA. Devem ser desenvolvidas soluções para aplicar a tecnologia no melhor interesse da sociedade.

Ao reconhecer os limites tecnológicos, os advogados encontrarão uma maior clareza sobre sua profissão e sua "bússola ética". “E descobriremos [...] que nossa experiência intuitiva, irredutível a regras, joga o peso do lado da mente humana enquanto tentamos estabelecer um novo equilíbrio entre nós e nossos ainda mais poderosos, embora talvez perpetuamente limitados, máquinas” (WISCHMEYER, 2018).

Em última análise, a regulamentação de tecnologia legal requer um intrincado ato de equilíbrio, especialmente entre os interesses dos consumidores relacionados à privacidade e os interesses econômicos dos desenvolvedores de software. Além disso, os reguladores devem levar em consideração os efeitos da regulamentação sobre a inovação, bem como as implicações da mudança técnica na lógica e no desenho da regulamentação.

A interação entre regulamentação e inovação é mútua e dinâmica. No entanto, as propostas sobre "proteção legal desde o projeto" apresentadas neste artigo fornecem um equilíbrio apropriado. Deve-se enfatizar, entretanto, que “proteção legal desde o design” deve ser exigida por lei, ou como Hildebrandt corretamente coloca: “A proteção legal desde o desenho” deve ser transformada de uma escolha ética em um requisito legal, então, poderemos ter certeza de que a

tecnologia legal será efetivamente alinhada com o estado de direito (Hildebrandt, 2017).

6 CONSIDERAÇÕES FINAIS

O estado é importante se quisermos criar tecnologias que beneficiem a população em geral. A tecnologia jurídica pode ser alinhada com o estado de direito apenas por meio da lei. Desse modo, o foco do projeto tecnológico deve estar na proteção da privacidade, se estivermos dispostos a construir sistemas que salvaguardem a liberdade humana. Além disso, precisamos desenvolver "mecanismos não apenas para maior transparência algorítmica, mas também para controle. Isso irá gerar confiança que é, aliás, um ingrediente essencial para o comércio e uma sociedade florescente. Portanto, se estamos nos esforçando para melhorar o comércio, nossa busca por autodefinição e nossa sociedade em geral, precisamos de melhor proteção legal desde o início.

Legisladores e os juristas devem estar cientes de suas responsabilidades. Comunicação e pesquisa interdisciplinar são necessárias. Somente quando elas estão em vigor, os reguladores governamentais podem encontrar o equilíbrio certo entre os interesses relacionados à privacidade e os econômicos. Nesse sentido, “proteção legal desde o início” servirá ao Estado de Direito e os melhores interesses da sociedade. Se começarmos a pensar criticamente sobre IA de uma perspectiva interdisciplinar, a sociedade pode fazer uso dela. E, possivelmente, a sociedade será mais "humana" por meio da IA.

REFERÊNCIAS

Angwin J, Larson J, Mattu S, Kirchner L. Machine bias. ProPublica, New York, 2016. Disponível em: www. propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acessado: abr 2021.

Dressel J, Farid H The accuracy, fairness, and limits of predicting recidivism. Sci Adv 4(1): eaao5580. 2018. Disponível em:https://doi.org/10.1126/sciadv.aao5580

GARTNER IT GLOSSARY. Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data. Acessado: abr 2021.

Hartzog W. Privacy’s blueprint. Harvard University Press, Cambridge, 2018.

Hildebrandt, M. Saved by Design? The Case of Legal Protection by Design. Nanoethics 11, 307–311, 2017. Disponível em: https://doi.org/10.1007/s11569-017-0299-0 https://br1lib.org/book/5886246/bb54bc. Acessado: abr 2021.

Kleinberg J, Lakkaraju H, Leskovec J, Ludwig J, Mullainathan S. Human decisions and machine predictions, National Bureau of economic research. Working Paper 23180. 2017. Disponível em: www.nber. org/papers/w23180. Acessado: abr 2021.

Kranzberg M. Technology and history: Kranzberg's Laws. Technol Cult 27(3):544–560, 1986.

La Diega GN. Against the dehumanisation of decision-making – algorithmic decisions at the crossroads of intellectual property, data protection, and freedom of information. J Inellect Prop Inf Technol Electron Commerce Law 9(1):3–34, 2018.

Lessing L. Code: and other law of cyberspace, Version 2.0. Basic Books, New York, 2006.

Martini Heidelberg M. Algorithmen als Herausforderung für die Rechtsordnung. JuristenZeitung 72:1017–1072, 2017.

MCDANIEL, John L.M. and PEASE, Ken G. Predictive Policing and Artificial Intelligence. First published by Routledge, New York, NY, 2021.

Medina E. Rethinking algorithmic regulation. Kybernetes 44:1005–1019, 2015.Disponível em: https://doi.org/10.1108/K-02-2015-0052 Acessado: abr 2021.

O'Hara K. Smart contracts – dumb idea. IEEE Internet Comput 21(2):97–101. 2017. Disponível em: https://doi. org/10.1109/MIC.2017.48

Pasquale F. Secret algorithms threaten the rule of law. MIT Technology Review. 2017. Disponível em: www. technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law. Acessado: abr 2021.

Pfeifer J. The data-driven lawyer and the future of legal technology, 2018. Disponível em: www. lawtechnologytoday.org/2018/01/the-data-driven-lawyer. Acessado: abr 2021.

Rademacher T. Predictive Policing im deutschen Polizeirecht. Archiv des öffentlichen Rechts 142:366–416, 2017.

Susskind R. Tomorrow's Lawyers: an introduction to your future. Oxford University Press, Oxford, 2013.

Ventura, Leonardo Henrique de Carvalho. Privacy by Design e Compliance na LGPD. 2021.Disponível em: https://jus.com.br/artigos/69585/privacy-by-design-e-compliance-na-lgpd. Acessado: abr 2021.

Vieira, Oscar Vilhena. Estado de Direito – Verbete. 2021. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/78/edicao-1/estado-de-direito. Acessado: abr 2021.

Wagner J. Legal Tech und Legal Robots: Der Wandel im Rechtsmarkt durch neue Technologien und künstliche Intelligenz. Springer, Wiesbaden, 2018.

Wischmeyer T. Regulierung intelligenter Systeme. Archiv des öffentlichen Rechts 143:1–66, 2018.

MÁQUINAS ROBÓTICAS E RESPONSABILIDADE CIVIL NO ÂMBITO DA UNIÃO EUROPEIA (UE)

Marcel Silva Luz[1]
José Carlos Ferreira da Luz[2]

1 INTRODUÇÃO

A concepção legal de uma máquina robô como um produto levou à aplicação de regras de responsabilidade civil para os produtores. No entanto, alguns aspectos da regulamentação europeia relevante sugerem que deve ser dada atenção especial a uma revisão neste domínio em relação à robótica. Tipos de defeito, significados do termo 'produtor', teste de expectativa do consumidor e dano imaterial são alguns dos aspectos que podem suscitar debates futuros. A inadequação da atual Diretiva 85 / 374 /EEC para regular os danos causados por robôs, especialmente aqueles com capacidade de autoaprendizagem, é destacada pelo documento 'Acompanhamento da Resolução do Parlamento da UE, de 16 de fevereiro de 2017, sobre as regras de direito civil sobre robótica'. Outros documentos relevantes são o Relatório sobre "Responsabilidade por IA e outras tecnologias digitais emergentes" preparado pelo Grupo de Especialistas em Responsabilidade e Novas Tecnologias, o "Relatório sobre as implicações de segurança e responsabilidade da Inteligência Artificial, Internet das Coisas e Robótica" [COM (2020) 64 final, 19/02/2020] e o *White Paper* "Sobre Inteligência Artificial - Uma abordagem europeia à excelência e confiança" [COM (2020) 65 final, 19/02/2020].

2 MÁQUINAS ROBÔS E ROBÔS VIRTUAIS

Costumávamos imaginar um robô, por causa do estereótipo apresentado nos filmes, como uma 'Máquina', com forma antropomórfica (um androide), dando a impressão de que eles agiriam ou pelo menos pareceriam agir de forma autônoma e interagir com os seres humanos. No entanto, os robôs são algo mais do que isso ou pelo menos do ponto de vista tecnológico, eles são muito mais do que são considerados pelo imaginário coletivo. Assim, dependendo do que é entendido pela

[1] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).
[2] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).

palavra 'robô' - e como um robô é representado - regras específicas irão regular os robôs. Portanto, do ponto de vista legal, nem todos os casos relacionados a robôs devem ser tratados da mesma maneira.

2.1 A DEFINIÇÃO DE UM ROBÔ

A definição 'tecnológica' comum de robô que abrange todas as situações é um sistema que é capaz de perceber o ambiente ou contexto em que está localizado, que pode processar a informação para planejar uma determinada ação e executá-la inclui máquinas robôs e entidades de inteligência artificial (LOOS, 2016).

O primeiro grupo de robôs, ou seja, máquinas robô englobam, por exemplo, um braço mecânico que coleta peças em uma linha de montagem e é empregado na indústria automotiva, ou uma máquina autônoma para uma finalidade específica seguindo as instruções fornecidas por algum software. O segundo grupo de robôs, inclui uma gama de casos que têm um elemento comum: um algoritmo escrito em código binário que pode atuar em resposta a um propósito predefinido ou que pode decidir de forma autônoma. As decisões e ações correspondentes não podem ser previstas pelo ser humano ou grupo de indivíduos que criaram o algoritmo (CURTIS, 2013).

Esses sistemas autônomos são chamados de 'agentes' 7 e podem se comunicar uns com os outros no que é denominado comunicação máquina a máquina (M2M). Eles parecem possuir vida, podendo analisar uma quantidade estonteante de dados, quase inimagináveis para o cérebro humano, encontrando diagnósticos relacionados ao câncer, bem como encontrando os melhores tratamentos possíveis com um grau de sucesso comparável ao de um especialista na área (MILLAR, 2013).

Uma vez que a inteligência artificial pode ser aplicada em todos os campos do conhecimento, há muitos outros exemplos em este grupo de robôs, incluindo drones e veículos completamente autônomos. Eles podem responder a softwares pré-projetados ou podem 'pensar' por si mesmos, processando informações que coletam continuamente do ambiente, da comunicação M2M e de bancos de dados (autoaprendizagem), graças à tecnologia que é a base da internet das coisas. Esse

tipo de conexão entre os agentes é denominado 'sistema multiagente' ou 'sociedade agente' (PERRITT, 2015).

Existem, portanto, três atividades fundamentais que um sistema deve desenvolver para ser considerado um robô. Em primeiro lugar, deve perceber - que é, deve reunir informações sobre o seu contexto, estando equipado com um sofisticado sistema de sensores. As informações coletadas devem ser processadas rapidamente para evitar que o sistema falhe. Deve-se observar que a máquina geralmente possui diferentes sensores, cada um dos quais coleta dados específicos que podem estar em conflito ou mesmo opostos a outras informações capturadas. Os algoritmos são responsáveis por acomodar todo tipo de informação e estabelecer um sistema completo e preciso que permita à máquina realizar ações eficientes e seguras para minimizar os danos que possam ocorrer. Em segundo lugar, o sistema deve planejar. Quando o algoritmo processa e analisa o ambiente, ele cria uma série de ações que são encomendadas para atingir objetivos específicos. Planejar também significa levar em conta as informações percebidas para selecionar ações ou determinar situações ou comportamentos que devem ocorrer no futuro.

Além disso, a escolha entre diferentes comportamentos e, portanto, o planejamento de ações futuras, deve ser feita o mais rápido possível para permitir que o sistema responda, por exemplo, em milissegundos a qualquer circunstância externa. Por último, o sistema deve atuar, ou seja, executar o plano previsto, para o qual a máquina costuma possuir um sistema eletrônico diferente do sistema mecânico e hidráulico tradicional que antes era empregado. Ações e comportamentos modificam e transformam o ambiente em que a máquina está localizada (CURTIS, 2013).

2.2 NOÇÃO ESTRITA DE UM ROBÔ

‘Um “robô” estritamente falando seria apenas aquele que tem capacidade de autoaprendizagem para que o programa não aplique apenas a heurística humana; caso contrário, a máquina cria seu próprio quadro heurístico de referências'. Esses robôs são conhecidos como 'robôs inteligentes' ou ‘Robôs especialistas’. De acordo com esta definição, diríamos que uma máquina dirigida por uma pessoa usando um controle remoto, como no caso de alguns drones ou carros sem motorista, nos quais

o ser humano deve estar presente para realizar certas tarefas ou para assumir o controle do veículo em circunstâncias específicas para as quais o veículo não está equipado para responder convenientemente, não pode ser considerado, no sentido adequado, um robô (FUNKHOUSER, 2018).

Um robô pode ter tamanhos diferentes, de um veículo a um chip (um nanorrobô), variando qualquer máquina que possua os três recursos descritos acima. Assim, existem máquinas robóticas e robôs virtuais. Os primeiros podem apresentar diferentes graus de mobilidade: podem ser completamente autônomos (como robôs assistivos ou sociais) ou não autônomo (por exemplo, um braço cirúrgico). Em geral, devem apresentar um nível mínimo de autonomia para responder a estímulos externos. Portanto, eles devem ter um certo grau de capacidade de tomar decisões (FUNKHOUSER, 2018).

Não podemos considerar ciborgues, próteses robóticas que uma pessoa pode carregar (por exemplo, um exoesqueleto) ou outras máquinas que são controladas remotamente, como robôs. Uma impressora 3D também não é um robô, embora utilize um software. No entanto, as impressoras 4D, que estão sendo pesquisadas na indústria, podem ser classificadas como máquinas inteligentes, pois permitem que materiais ou produtos se adaptem permanentemente ao meio ambiente, redesenhando-se ao mesmo tempo. Este tipo de impressora está mais próximo da ideia de um robô do que de uma impressora 3D pura (CASINI, 2018).

Por outro lado, surgem dúvidas quando um ser humano especialista e um especialista robô não tem a mesma opinião depois de analisar uma determinada situação ou dados e tomar decisões opostas. Qual deles dedicou mais atenção à análise? O robô ou o humano? Se decidirmos seguir a decisão de um deles e essa decisão não for a correta, e se agir de acordo com essa decisão causar danos a terceiros, quem será considerado responsável?

Se um robô inteligente é projetado para atender a propósitos específicos pré-determinados, ele é chamado de 'robô fechado', ao passo que se não for limitado em seus propósitos, pode mudar seu comportamento e, portanto, realizar diferentes trabalhos dependendo de o ambiente e tomar decisões que poderiam ser julgadas por um indivíduo como imprevisíveis, usando um código *'open-source'*, o robô inteligente é chamado de *'open-source*' robô'. Neste caso, as alterações podem

ser feitas no sistema por terceiros sem comprometer o desempenho das tarefas (CALO, 2021).

Máquinas robôs e robôs virtuais podem ser robôs fechados ou abertos, embora os primeiros sejam frequentemente robôs fechados (por exemplo, robôs para a indústria), enquanto os últimos são geralmente robôs abertos.

2.3 NOÇÃO EUROPEIA DE ROBÔ

A noção europeia de máquina robótica parece ser definida pela atribuição de cinco características: (i) aquisição de autonomia através de sensores ou troca de dados com o ambiente (interconectividade), bem como a comercialização e análise desses dados; (ii) capacidade de aprender (autoaprendizagem) com a experiência e pela interação com outros robôs (M2M); (iii) uma pequena presença física, para distingui-lo de um robô virtual; (iv) adaptação de seu comportamento e ações ao meio ambiente; e (v) ausência de vida biológica. De acordo com esse conceito de robô, podemos diferenciar três grupos de robôs inteligentes: (i) sistemas ciberfísicos, (ii) sistemas autônomos e (iii) robôs autônomos inteligentes (PARLAMENTO DA EU, 2017).

Para os formuladores de políticas da UE, dois critérios definem um robô: primeiro, a noção estrita de um robô, conforme descrito acima, e, segundo, ser uma máquina robô que pode ser considerada como tendo o status de pessoa eletrônica responsável por qualquer dano que cause. No entanto, a atribuição de personalidade jurídica é, na verdade, uma questão muito controversa.

3 ROBÔS SOB UMA PERPECTIVA LEGAL

3.1 QUADRO LEGAL ATUAL

Devido à diversidade de tipos de robô, não existe uma estrutura legal única para todos eles. Ou seja, um androide não merece a mesma consideração jurídica que um braço cirúrgico, ou como um sistema operacional que pode tomar decisões de forma autônoma, como um robô consultor ou um agente eletrônico que pode fechar contratos e escolher sua contraparte.

As regras relativas à responsabilidade por danos causados por robôs estão relacionadas ao entendimento legal dos mesmos. Por outro lado, é importante atentar para o fato de que a maioria dos robôs contém um sistema operacional, um programa de computador. Por outro lado, devemos levar em conta que os robôs têm sido empregados no mundo real, interagindo com as pessoas como robôs assistentes, robôs enfermeiros ou drones, ou em meios de transporte autônomos em geral. Assim, além da responsabilidade do fabricante da máquina robô, existe a responsabilidade do proprietário do robô e a responsabilidade do projetista-engenheiro.

Ao estudar esses tópicos, é importante lidar com máquinas robóticas e robôs virtuais separadamente. Como os robôs virtuais são programas de computador, as regulamentações relacionadas a programas de computador devem ser aplicadas a eles. As máquinas robóticas podem ser consideradas como um "bem móvel", uma das diferentes partes da qual poderia ser um programa de computador (por exemplo, drones ou carros sem motorista). Não obstante, quando um robô faz parte de um bem móvel ou imóvel, ele pode ser visto, na classificação tradicional de bens, como um 'bem imóvel' por destino ou por incorporação, dependendo do caso particular tratado (por exemplo, braços cirúrgicos30 ou braços da indústria automotiva).

3.2 REGULAMENTO DO PROJETO E PRODUÇÃO DE MÁQUINAS ROBÔ

A regulamentação do projeto e da produção de máquinas robóticas por meio de normas técnicas é uma das áreas em que a lei pode ter efeito, ao exigir certos níveis de proteção e segurança para minimizar os riscos para os seres humanos que manuseiam essas máquinas, especialmente os chamados robôs colaborativos. Nestes casos, o robô não é uma mera ferramenta ou assistente do indivíduo, mas colabora com ele, realizando determinada tarefa da mesma forma que poderia ser realizada por duas pessoas, ou mesmo de uma maneira melhor. Os requisitos de segurança devem ser levados em consideração no projeto e na produção subsequente do robô.

Um robô para a indústria é considerado uma 'máquina'. Portanto, a Diretiva 2006/42 / EC do Parlamento Europeu e do Conselho de 17 de maio de 2006 (conhecida como Diretiva de Máquinas) e que altera a Diretiva 95 / 16 / EC32 se

aplicam a ela. Esta diretriz define os requisitos essenciais de saúde e segurança para aplicação geral, complementados por uma série de requisitos mais específicos para certas categorias de máquinas. A máquina deve ser projetada e construída de modo que seja adequada para sua função e possa ser operada, ajustada e mantida sem colocar as pessoas em risco, tanto quando essas operações são realizadas nas condições esperadas, mas também levando em consideração qualquer razoavelmente uso indevido previsível do mesmo (EUROPEAN COMMISSION, 2018).

No plano internacional, existem as conhecidas normas ISO que, no domínio dos robôs industriais, são particularmente tidas em conta pela UE e pelos Estados-Membros. ISO 10218-I e 10218-II foram revisados e atualizados pela ISO 15066: 2016. Outros padrões ISO relevantes são ISO 26262, relativos à segurança no campo de veículos, e ISO / IEC 15288, em relação a sistemas de engenharia e Programas. Em relação aos robôs terapêuticos ou assistentes que acompanham menores durante o tratamento médico, auxiliam pessoas com deficiência nas atividades diárias ou auxiliam idosos em suas casas, é previsível que o ser humano tenha contato físico com o robô ou que sua casa deve ter certas dimensões ou outros requisitos específicos. Certos padrões de segurança devem, portanto, ser estabelecidos, bem como mecanismos que, em certas situações, possam desligar automaticamente o sistema robótico para evitar que sejam causados danos. O projeto deve, portanto, enfatizar a capacidade do robô de cumprir certos requisitos legais e até sociais. O documento ‘Acompanhamento da Resolução do Parlamento da UE de 16 de fevereiro de 2017 sobre as Regras de Direito Civil sobre Robótica’ recomenda que este tipo de robô (um robô assistente ou colaborativo) receba uma consideração especial e menciona sua possível regulamentação futura. Por esse motivo, foram constituídos comitês técnicos especializados, como o Comitê de Robótica ISO / TC 299, que se dedica exclusivamente ao desenho de regras relacionadas com a robótica. Nesse sentido, a ISO 13482: 2014 deve ser levada em consideração (ISO, 2021).

Além disso, o contexto em que o robô executa sua atividade autônoma pode exigir que ele respeite certas regras legais que podem, como as normas técnicas, afetar sua atividade por meio do projeto do sistema de inteligência artificial embutido nele. É o caso dos carros sem motorista, que devem dar atenção especial às regras

de trânsito e segurança, bem como às de responsabilidade. Atualmente, os pesquisadores trabalham com algoritmos que permitem que eu agentes inteligentes para reconhecer as normas e respeitá-las, adaptando-se ao contexto incerto e sempre mutante no qual eles interagem. Porque, nesses casos, estamos lidando com robôs assistentes, e não industriais, do ponto de vista jurídico, o produtor deve levar em consideração outras regras, em particular a Diretiva 2001 / 95 / CE do Parlamento Europeu e do Conselho de 3 de dezembro, sobre a segurança geral dos produtos, e a Diretiva do Conselho 85 / 374 / CEE de 25 de julho 1985 na aproximação das leis, regulamentos e administrativos disposições dos Estados Membros relativas à responsabilidade por produtos defeituosos (EUR-LEX, 2021)

Outros casos interessantes são as regras relativas ao respeito ou à adaptação ao meio ambiente através, por exemplo, de canalização ou de infraestruturas inteligentes que aproveite as vantagens da nanotecnologia e da impressão 4D.

Perto do domínio da robótica estão as interfaces cérebro – computador, que consistem em sistemas artificiais que interagem com o sistema nervoso por meio de sinais neurofisiológicos e são usados, por exemplo, por pessoas com deficiência durante a execução de certas atividades motoras. Os ciborgues são um campo em que essas interfaces podem ter aplicação completa. É importante ter presente que o dever de informar, para que uma pessoa dê consentimento informado à implantação do sistema artificial em questão, é imposto pelos ordenamentos jurídicos nacionais (RIBES et al., 2021).

Em suma, se um robô ou um artefato autônomo for colocado no mercado, as regras legais podem determinar não apenas sua estrutura corporal, mas também suas capacidades, por meio do projeto do próprio sistema de inteligência artificial. Para isso, é útil que sensores que permitem a recepção de informações do ambiente sejam incorporados de forma que o robô seja capaz de se adaptar às mudanças de circunstâncias.

4 A RESPONSABILIDADE DOS PROPRIETÁRIOS DE UM ROBÔ: ALGUMAS REFLEXÕES

Uma questão central na robótica é a distribuição de responsabilidade entre humanos e robôs ou outras máquinas inteligentes quando eles causam danos a

terceiros. Embora esta questão seja o assunto de outro capítulo neste volume, não posso resistir a levantar a questão da responsabilidade do dono de um robô. Dependendo do grau de mobilidade ou da autonomia de decisão do robô, os danos causados a outra pessoa podem estar sujeitos a várias regras específicas. No caso de um androide, pode ser considerado um menor e, consequentemente, a responsabilidade do proprietário, então a responsabilidade seria de um pai ou responsável, ainda que por analogia? No caso de um robô de estimação, então, seria melhor aplicar a responsabilidade objetiva por danos causados por animais? (CALO, 2015).

A aplicação da Diretiva 2001 / 95/ CE, relativa à segurança geral do produto, seria suficiente? Talvez um robô deva ser considerado um gênero tertius da mesma forma que os animais em alguns sistemas jurídicos nacionais, como os da Alemanha, Suíça ou Áustria. Quando a máquina de robô é usada por um fornecedor de serviços, alguém poderia tratar sua responsabilidade por danos como responsabilidade indireta da mesma forma que um principal é responsável por danos causados por assistentes?

Na opinião de Calo (2015), esta opção sugere que máquinas de robô e funcionários têm o mesmo estatuto jurídico, o que é duvidoso. O fato de desempenharem funções semelhantes não significa que mereçam igual consideração legal.

Embora não acredite que uma regra específica seja necessária para regular a responsabilidade no caso de possuir um robô, os legisladores devem alterar os códigos civis para regular a responsabilidade civil pela posse de mercadorias potencialmente perigosas, incluindo robôs ou artefatos inteligentes. Se isso for considerado com base na culpa (com possível presunção iuris tantum de falta de diligência, como nos casos relativos à responsabilidade dos pais ou tutores pelos atos de menores sob sua responsabilidade) ou de responsabilidade objetiva (como no caso de animais ou do manejo de máquinas potencialmente perigosas), obtendo seguro com um nível mínimo de cobertura para os danos causados pelo robô deve ser obrigatório. Não concordo com a ideia sugerida por alguns estudiosos de que, embora terceiros devam ser indenizados pelo proprietário, a responsabilidade deve ser atribuída à própria máquina (CALO, 2015)

Nesse caso, a máquina seria considerada uma criança, ou seja, uma pessoa humana, ou, pelo menos, personalidade jurídica seria atribuída a ela. Ainda não é o caso, embora possa se tornar o caso no futuro por meio de decisões de formuladores de políticas nacionais. Em minha opinião, se a atribuição a um robô da consideração de "titular de direitos e deveres" faz algum sentido, é o de ser capaz de ser “O sujeito” ao qual é “atribuída” a ação causadora do dano, enquanto “o sujeito” que há de ser considerado “responsável” é o humano. Assim, seria um (novo) caso de responsabilidade civil por ato alheio.

4 RESPONSABILIDADE DO PRODUTOR POR DANOS CAUSADOS POR UMA MÁQUINA DE ROBÔ: REVISÃO

As preocupações sobre o manuseio responsável de robôs inteligentes levaram o Parlamento Europeu à emissão de uma Resolução em 31 de maio de 2016, apresentando uma proposta sobre a matéria à Comissão encarregada de redigir as normas de direito civil. Esta proposta foi seguida, por um lado, do Relatório com Recomendações à Comissão de Normas de Direito Civil sobre Robótica e, por outro lado, o Acompanhamento do Parlamento da EU.

Resolução de 16 de fevereiro de 2017 sobre as Normas Civis de Robótica. Esses dois documentos também enfocam a necessidade de regulamentar a responsabilidade civil por danos causados por robôs. A resolução do Parlamento Europeu de 12 de fevereiro de 2019 sobre uma política industrial europeia abrangente em inteligência artificial e robótica (2018/2088 (INI)), o relatório sobre "Responsabilidade por IA e outras tecnologias digitais emergentes" preparado pelo Grupo de Peritos em Responsabilidade e Novas Tecnologias”, em que se destaca a necessidade de revisão das regras de responsabilidade, também devem ser tidas em consideração (LOOS, 2017).

Embora a compensação por danos causados por defeitos em robôs e outras máquinas inteligentes possa ser concedida de acordo com a legislação nacional de responsabilidade do produtor, questões clássicas relacionadas à aplicação desta legislação a tais 'produtos' surgirão quando se trata de revisões futuras desta legislação. J2 Na verdade, a inadequação de a atual Diretiva 8J / 374 / CEE para regulamentar os danos causados por robôs, principalmente aqueles com capacidade de autoaprendizagem, é destacado pelo documento de 'Acompanhamento'

mencionado acima. J3 Alguns tópicos para uma possível revisão futura da legislação da UE sobre responsabilidade do produtor são apresentados abaixo (Loos, 2017).

4.1 MÁQUINAS ROBÔ COMO PRODUTOS

Uma máquina robô pode ser incluída na definição de 'produto'. Portanto, o produtor de um robô pode ser considerado responsável por defeitos que causem danos a outrem. Para efeitos da Directiva 85/ 374 / CEE, o artigo 2.º estabelece que “produto” significa “todos os bens móveis, com exceção dos produtos agrícolas primários e de caça, ainda que incorporados noutro móvel ou imóvel”.

De acordo com a visão legal de uma máquina robótica, adotada nesse artigo, podemos afirmar que os robôs podem ser legalmente considerados produtos e que as regras da Comunidade Europeia devem ser aplicadas. Normalmente, uma máquina robô (um bem tangível) incorpora o software de uma forma que dificulta a distinção entre software e o bem, por exemplo, nos casos em que o software é necessário para o funcionamento do robô. Nesse caso, é geralmente aceito que o programa de computador se torne uma parte inseparável do robô ao qual está incorporado. Portanto, deve ser tratado como um produto que se enquadra no âmbito da diretiva, dada a ligação entre a máquina robô e o programa de computador.

Dado que os robôs estão se tornando cada vez mais sofisticados, o 'estado de conhecimento científico e técnico existente no momento em que ele colocou o produto (o robô) em circulação' é especialmente relevante para avaliar a defesa do produtor contra a responsabilidade (Artigo 7 (e) da Diretiva 85 / 374 / CEE). As atualizações e upgrades de software questionam a aplicação da chamada “exceção de riscos de desenvolvimento”.

4.2 TIPOS DE DEFEITOS

Em primeiro lugar, porque as máquinas robóticas estão se tornando cada vez mais sofisticadas, podemos levar seus projetos em particular em consideração, de modo que os defeitos que significam que o robô é considerado "defeituoso" são defeitos de projeto com mais frequência do que defeitos de fabricação.

Por sua vez, o grau de sofisticação implica que deve haver mais precisão nos avisos, informações e instruções que o produtor deve fornecer ao comprador do robô; ou seja, deve haver mais informações, mas também as informações devem ser mais técnicas. Algum tipo de conhecimento específico é mesmo necessário ao usuário do robô ou máquina inteligente, se ele quiser ter um entendimento completo das informações e instruções fornecidas. A complexidade desta informação e destes as instruções sugerem que, no futuro, a falta de informação se tornará um defeito mais comum do que é hoje. Consequentemente, defeitos no projeto e nas instruções serão o tipo de defeito que os robôs apresentarão com frequência, em vez de defeitos de fabricação (WUYTS, 2021).

Desta declaração, segue-se que, se o produtor for considerado responsável em qualquer caso de acordo com a legislação atual, seu próprio investimento em alta tecnologia poderia ser consideravelmente reduzido. Na busca do equilíbrio entre o investimento em pesquisa tecnológica e a responsabilidade perante terceiros, a solução não deve ser proteger o fabricante se houver certos defeitos.

Como proposto por Ryan Calo, a melhor solução seria para definir os critérios de imposição e responsabilidade civil ao produtor de acordo com o tipo de defeito. Consequentemente, a responsabilidade objetiva seria a melhor regra em relação aos defeitos de fabricação, enquanto a presunção de falha iuris tantum seria mais apropriada para os defeitos de projeto e de informações / instruções. Não obstante, a proposta do Parlamento Europeu a Comissão para a regulamentação dos robôs e o Relatório de Responsabilidade por Inteligência Artificial optam claramente pela introdução da responsabilidade independente de culpa por parte do fabricante do robô em todos os casos relativos a defeitos (CALO, 2015).

Além disso, a proposta estabelece que o proprietário de um robô deve fazer um seguro obrigatório para danos causados a outrem e exige a criação de um fundo de compensação que cubra todos os danos que não possam ser cobertos por esse seguro (EU PARLIAMENT, 2017).

4.3 NOÇÃO DE PRODUTOR: A REGRA DE "RESPONSABILIDADE PELA PARTICIPAÇÃO NO MERCADO"

A definição de quem legalmente deve ser considerado o ‘produtor’ merece atenção especial. Nos termos do artigo 1.º da Diretiva 85 / 374 / CEE, o produtor é

considerado responsável pelos danos causados a terceiros por defeito do seu produto. Alguns estudiosos argumentam (embora sem fornecer dados para apoiar esta visão) que se o produtor é exclusivamente responsável, mesmo quando o defeito não é propriamente um defeito em fabricação e, além disso, é responsável se houver um defeito no design quando, por exemplo, vários indivíduos estiveram trabalhando no produto (por exemplo, o criador do algoritmo, o programador, o designer e o fabricante de uma determinada parte) ou um grupo ou equipe de pesquisa está envolvido, uma certa falta de interesse no investimento na fabricação de robôs ou outras máquinas inteligentes poderia ser justificado (HUBBARD, 2015).

Se levarmos em consideração o fato de que a maioria dos defeitos que podem ser encontrados em robôs ou outras máquinas inteligentes são defeitos no design ou concepção do 'produto', vale a pena sugerir uma definição mais ampla de 'produtor' que inclui o engenheiro e / ou projetista do robô, desde que não trabalhem para o fabricante (ou seja, não façam parte da estrutura da empresa do fabricante). Como se sabe, o projetista de um produto que não é o fabricante ou o reparador está fora do escopo da noção de produtor. No entanto, o projetista pode ser responsabilizado diretamente como fabricante de um componente do robô pelos danos causados.

Em qualquer caso, uma pessoa lesada pode intentar uma ação civil direta por danos contra o engenheiro ou o projetista, de acordo com as regras nacionais em vigor sobre responsabilidade civil, na medida em que o artigo 13 da Diretiva 85/ 374 / CEE afirma que “esta diretiva não afetará quaisquer direitos que um pessoa lesada pode ter de acordo com as regras da lei de contratos ou não responsabilidade contratual ou um regime de responsabilidade especial existente no momento da notificação da presente diretiva”. No relatório do NTF (Grupo de Peritos em Responsabilidade e Novas Tecnologias), o “projetista” do sistema de IA pode ser considerado um operador de *backend*.

Como já enfatizado, é um lugar comum usar software livre na criação de um robô (um robô aberto) e, neste caso, qualquer pessoa pode apresentar mudanças ou inovações ou adicionar padrões específicos a protocolos públicos, e assim por diante. A incerteza sobre a pessoa ou pessoas que agem afetam a existência e a prova da 'relação causal' entre o defeito e o dano. Portanto, embora ainda possa ser

criticada, a regra de responsabilidade de participação de mercado deve receber consideração primordial (CALO, 2015).

Em 1999, foram levantados aspectos relacionados com a prova do dano, o defeito e a relação causal, entre outras questões, no *Green Paper* apresentado pela Comissão sobre a responsabilidade por produtos defeituosos. *Green Paper* são documentos publicados pela Comissão Europeia para estimular o debate sobre determinados temas a nível europeu. Convidam as partes relevantes (órgãos ou indivíduos) a participar num processo de consulta e a debater com base nas propostas que apresentam. Os *Green Paper* podem dar origem a desenvolvimentos legislativos que são então descritos no *White Paper.*

Uma das propostas era a aplicação da referida regra de quota de mercado responsabilidade, com vista a uma possível alteração da Diretiva 85 / 374 / CEE. Os aspectos considerados incluíram: (i) a presunção legal da relação causal quando o lesado comprovar o defeito e o dano; (ii) a presunção legal do vício quando o lesado provar a existência do dano; (iii) obrigar o produtor a fornecer todo o tipo de documentação e informação útil para que o lesado possa beneficiar de elementos específicos de prova dos factos (regra de descoberta); e (iv) exigir que o produtor pague os custos dos peritos, a fim de aliviar o ónus da prova por parte da pessoa lesada, sob certas condições - por exemplo, a pessoa lesada pode pedir o juiz ordene ao produtor que pague as despesas necessárias para a vítima provar seu caso, desde que a vítima reembolsasse as despesas (mais, possivelmente, juros) se a reclamação não fosse bem-sucedida. A comunicação M2M pode estabelecer uma causalidade natural entre os tipos de defeito e o dano de forma muito mais clara, atendendo ao critério de imputação objetiva que deve ser levado em consideração pelos juízes (CALO, 2015).

Na internet das coisas, as máquinas inteligentes se comunicam diretamente com o fabricante, projetista ou programador, indicando problemas, deficiências ou defeitos. A comunicação M2M é, de fato, utilizada atualmente por muitas empresas. Em qualquer caso, a digitalização e a IoT permitem rastrear o comportamento das coisas e armazenar todas essas informações no que se chama de “caixa preta”. O acesso a ela por parte dos lesados pode facilitar o fardo de provar o defeito.

Nessas circunstâncias, e com economia significativa de custos, o agente causador do dano pode ser totalmente identificado, e esse tipo de comunicação

pode levar a uma mudança significativa nas regras atuais sobre a responsabilidade do fabricante. Com base em sistemas especialistas, defeitos de qualquer tipo que apareçam podem ser totalmente identificados e corrigidos quase imediatamente, pelo menos se o sistema for capaz de se reparar, ou se o mecanismo defeituoso puder ser interrompido, o que pode prevenir ou minimizar os danos.

O conhecimento do defeito que é imediatamente adquirido pelo responsável permite-lhe tomar medidas urgentes a este respeito (por exemplo, modificar o software ou alertar o utilizador sobre o possível risco de danos e as melhores medidas para evitá-lo). Vale ressaltar que as questões levantadas sobre a responsabilidade do produtor após a entrada em circulação do produto, no que diz respeito à identificação de um defeito que possa causar dano, devem ser respondidas de acordo com as regras gerais de responsabilidade civil de direito interno (GIORGIO, 2019).

4.4 O TESTE DE EXPECTATIVAS DO CONSUMIDOR

O teste de expectativas do consumidor deve ser considerado em uma futura revisão da Diretiva 85 / 374 / CEE (Art. 6). A este respeito, seria aconselhável levar em consideração os critérios que foram propostos em relação à Reapresentação (Terceiro) dos Delitos nos EUA, e para aplicar o teste de design alternativo razoável em vez do teste de expectativas do consumidor. O teste de design alternativo razoável foi criticado com o fundamento de que favorece excessivamente o fabricante (o empresário), impondo custos excessivos ao consumidor (especialmente em relação à prova do defeito), uma vez que levam em consideração os testes 'riscos-utilidade '. No entanto, uma vez que a comunicação entre máquinas inteligentes está avançando, pode não ser insensato levar este teste em consideração, mesmo que ambos os testes sejam aplicados em conjunto com o propósito de determinar se uma máquina inteligente está com defeito ou não, ou, acima de tudo, se acreditarmos que os defeitos estão mais no design do que na fabricação (CAUFFMAN, 2018).

Além disso, se um design alternativo razoável existe ou não é uma questão que um algoritmo será capaz de responder - ou já pode responder - uma vez que os

dados aos quais a comunicação M2M deu origem tenham sido tratados. Haveria total cumprimento, nesses casos, da neutralidade tecnológica.

4.5 INCLUSÃO DE DANOS IMATERIAIS

Os danos imateriais (danos morais e outras perdas imateriais) foram tradicionalmente excluídos da proteção estendida pela Diretiva 85 / 374 / CEE, no sentido de que a existência e o âmbito da obrigação de indemnizar são determinados exclusivamente pelas regulamentações domésticas. Em primeiro lugar, precisamos determinar o significado de "dano imaterial". De acordo com alguns estudiosos, apenas danos para o qual a indenização não pode ser concedida deve ser considerada como dano imaterial, porque apesar de uma quantia de dinheiro sendo recebida pela pessoa lesada, a utilidade que a pessoa lesada tinha antes do dano ocorrido não é restaurada. Portanto, se a compensação restaura a utilidade da pessoa lesada, o dano causado deve ser tratado como dano material.

A intenção dos legisladores que elaboraram a diretiva em nome da Comunidade Europeia em 1985 deveria excluir os danos imateriais do âmbito da diretiva e remetê-los para a legislação nacional. Há também uma razão substantiva, que é que a Alemanha foi contra a regulamentação do dano imaterial a nível comunitário devido às diferenças de critérios entre os Estados-Membros e, em particular, aos critérios aplicados pelos tribunais nacionais no que diz respeito à admissão de indenização por tais danos (MARTÍN AND SOLÉ, 2003).

Com efeito, em meados da década de 1980, quando a diretiva estava a ser redigida, enquanto a indenização por danos imateriais era concedida de forma bastante livre (mesmo superficial) na França e na Espanha, a Alemanha não o permitia e a situação na Itália era muito restritiva. Hoje, desde a reforma do BGB (§ 253.2) em relação à responsabilidade civil impetrada pelo legislador alemão em 2002, os pedidos de indemnização por dano imaterial são admitidos, em geral, nos casos de lesão corporal, saúde, liberdade e autodeterminação sexual, e também no regime de responsabilidade objetiva (MAGNUS, 2003).

Na legislação de responsabilidade civil de produtos defeituosos, naquele mesmo ano, uma seção final foi introduzida no § 8 *Produkthaftungsgesetz* de 15 de dezembro de 1989, em virtude do qual a parte lesada só pode reclamar os danos

imateriais que uma lesão corporal causada por um defeito do produto lhes teria causado. Assim, a Diretiva 85 / 374 / CEE deve ser alterada para garantir que o dano imaterial seja abrangido pelo seu âmbito de proteção. Na verdade, a Resolução do Parlamento Europeu à Comissão, de fevereiro de 2017, sobre as normas em matéria de robótica, adverte que as normas sobre responsabilidade civil devem abranger todos os possíveis danos causados por um robô, dado, como já fez foi indicado que nem todos os casos que envolvem um robô se enquadram no âmbito da atual redação da diretiva (MAGNUS, 2003).

5 CONSIDERAÇÕES FINAIS

A internet das coisas, assim como os robôs e outras máquinas inteligentes, apresenta um desafio às normas de responsabilidade civil, fazendo surgir a necessidade de um sistema articulado que possa responder às novas situações que possam ocorrer. Não se deve esquecer que a comunicação permanente entre máquinas inteligentes, ou sistemas capazes de se autorreparar, ou robôs especialistas que tomam decisões em momentos críticos, pode reduzir drasticamente o número de acidentes ou mortes, com a consequente diminuição de mortes e lesões corporais com consequências a longo prazo. Isso pode ter um grande impacto econômico, não apenas no campo da saúde. O impacto será de particular importância no setor de seguros.

A comunicação permanente entre máquinas inteligentes pode permitir que as próprias máquinas se adaptem constantemente aos novos avanços técnicos e científicos ou se adaptem ao seu ambiente com base no conhecimento existente em um domínio específico ou para uma técnica específica. Isso inevitavelmente, mais cedo ou mais tarde, afetará as regras sobre a responsabilidade civil do produtor e proprietário de um robô ou máquina inteligente. A robótica, então, pode ser uma grande oportunidade para revisar e finalmente alterar diferentes aspectos das regras da Comunidade (EUR-LEx, 2018). Em qualquer caso, futuras informações "personalizadas" com base nas preferências do cliente, dados, necessidades, capacidades, por meio da análise de dados massivos armazenados pelo fabricante, podem permitir "personalizar" a responsabilidade evitando a aplicação de uma regra geral.

REFERÊNCIAS

Calo, Ryan, Open Robotics. Maryland Law Review, Vol. 70, No. 3, 2015, Disponível em: SSRN: https://ssrn.com/abstract=1706293. Acesso: mai 2021.

Calo, Ryan, Robotics and the Lessons of Cyberlaw (February 28, 2014). California Law Review, Vol. 103, No. 3, pp. 513-63, University of Washington School of Law Research Paper No. 2014-08. 2015. Disponível em: https://ssrn.com/abstract=2402972 or http://dx.doi.org/10.2139/ssrn.2402972. Acesso: mai 2021.

Casini, Marco. Smart Buildings: Advanced Materials and Nanotechnology to Improve Energy, Elsevier, 2016.

Cauffman, Caroline. Maastricht journal of European and comparative law. The article raises the question of how to deal with liability for AI and discussion some legislative proposals in this respect. 2018. Disponível em: https://doi.org/10.1177/1023263X18812333. Acesso: mai 2021.

Curtis E.A. Karnow. "The application of traditional tort theory to embodied machine intelligence," republished in ROBOT LAW (forthcoming Fall 2015) The SelectedWorks of Curtis E.A. Karnow. 2013.Disponível em: http://works.bepress.com/curtis_karnow/9. Acesso: mai 2021.

EU Parliament. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html#title1. Acesso: maio 2021.

Eur-Lex. At the time of writing, the abovementioned directive is being reviewed - Artificial Intelligence for Europe, SWD(2018) 237 final. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:137:FIN. Acesso: Mai 2021

Eur-Lex. Commission staff working document, 'Liability for emerging digital technologies', SWD/2018/137final. Disponível em: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137. Acesso em: mai 2021.

Eur-Lex. OJL 11/4, 15.1.2002. OJL 210, 7.8.1985. Disponível em: https://eur-lex.europa.eu/homepage.html. Acesso em: mai 2021.

Funkhouser, Kevin. 'Paving the Road Ahead: Autonomous Vehicles, Products Liability and the Need for a New Approach' 2013. Disponível em: https://www.scinapse.io/papers/1575317154#ref. Acesso em: 25 mai 2021.

Giorgio Risso Product liability and protection of EU consumers: is it time for a serious reassessment?, Journal of Private International Law, 2019. Disponível em: 10.1080/17441048.2019.1579994. Acesso: mai 2021.

Hubbard, F. Patrick. 'Sophisticated Robots: Balancing Liability, Regulation and Innovation' (2015) Disponível em:

https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1204&context=flr. Acesso: mai 2021.

ISO. Disponível em: <www.iso.org/obp/ui/#iso:std:iso:ts:15066:ed-1:v1:en>. Acesso: maio 2021.

Loos, Marco. Machine-to-Machine Contracting in the Age of the Internet of Things' in Schulze, Staudenmayer, and Lohsse (eds), Contracts for the Supply of Digital Content. Regulatory Challenges and Gaps Nomos Verlag. 2017. Disponível em: https://dare.uva.nl/search?identifier=6e464e82-0bee-4bc5-97f1-c94d9e6bfdc7. Acesso: mai 2021.

Magnus, Ulrich The Reform of German Tort Law. (2003) 4 InDret. Disponível em: <www.indret.com>. Acesso: mai 2021.

Martín and Solé, 'El daño moral' in Cámara (ed), Derecho Privado Europeo (Colex 2003) 859–860.

Millar, Jason and Kerr, Ian R., Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots, 2013. Disponível em: https://ssrn.com/abstract=2234645 or http://dx.doi.org/10.2139/ssrn.2234645. Acesso: Mai 2021

Perritt, H. H., & Sprague, E. O.. Law Abiding Drones. Science and Technology Law Review, 16(2), 2015. Disponível em: https://doi.org/10.7916/stlr.v16i2.3996.

Resolução do Parlamento da UE de 16 de fevereiro de 2017 sobre Regras de Direito Civil sobre Robótica, 2015/2103 INL. Disponível em; https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. Acesso: mai 2021.

Ribes, Cerquides, Demiris, and López de Mántaras. 'Active Learning of Object and Body Models with Time Constraints on a Humanoid Robot' IEEE Transactions on Autonomous Mental Development. 2016. Disponível em: https://www.researchgate.net/publication/279163131_Active_Learning_of_Object_and_Body_Models_with_Time_Constraints_on_a_Humanoid_Robot. Acesso: mai 2021.

Robert, 'Impresoras 3D y 4D' in Navas (ed) Inteligencia artificial. Tecnología. Derecho Tirant Lo Blanch, 2017.

Wuyts, Daily. "The Product Liability Directive – More than two Decades of Defective Products in Europe" Journal of European Tort Law, vol. 5, no. 1, 2014. Disponível em: https://doi.org/10.1515/jetl-2014-0001. Acesso: mai 2021

TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL E RESPONSABILIDADE EM SAÚDE DIGITAL

Patrícia Cristina Ferreira Moura[1]
Carlos Eduardo Leite Lisboa

1 INTRODUÇÃO

No Preâmbulo da Constituição da Organização Mundial da Saúde ('OMS'), saúde é definida como 'um estado de completo bem-estar físico, mental e social'. O direito à saúde é considerado um direito humano e agora está bem reconhecida no direito internacional, particularmente na Constituição da OMS de 1946 e na Declaração Universal dos Direitos Humanos de 1948 ((World Health, 2021).

A pandemia COVID-19, no entanto, desafiou sua implementação efetiva, sobrecarregando os sistemas de saúde, criando sofrimento, derrubando instituições internacionais e abrandando crescimento econômico. A pandemia também criou dilemas morais, especialmente para profissionais médicos e formuladores de políticas que enfrentam a escassez de recursos disponíveis em dispositivos respiratórios específicos e dados adequados sobre as consequências da pandemia. E evidenciou a questão do valor da vida humana em um contexto de escassez de recursos. Em suma, a pandemia COVID-19 demonstrou que os sistemas de saúde devem ser resilientes a surtos e estar mais bem preparada para prever e reagir a tal tragédia humana e econômica.

Nesse contexto, a questão é se uma grande quantidade de dados pessoais, de fontes multimodais, combinados com algoritmos de IA e aprendizado de máquina (*machine learning* (ML)), têm potencial para melhorar o acesso e a qualidade dos serviços de saúde para os usuários finais em uma perspectiva de custo-benefício. Na corrida por uma vacina, a Moderna, por exemplo, conseguiu usar os sistemas de IA de forma eficaz. Na verdade, a empresa usou dados estruturados para projetar algoritmos mais eficientes para apoiar a tomada de decisão no espaço clínico, onde fornecem previsões que os humanos não seriam capazes de fazer em um período de tempo razoável. (FROST & SULLIVAN, 2021).

[1] Universidade de Lisboa – UL. Faculdade de Direito. – FADUL. Alameda da Universidade 1649-014 Lisboa – Portugal. Università degli Studi Roma Tre - Dipartimento di Giurisprudenza -Via Ostiense 159, 00154 Roma-It

A Frost & Sullivan define Digital Health como a "aplicação de dados para a prestação de cuidados de saúde, usando tecnologias computacionais e de telecomunicações, para apoiar o fluxo de trabalho do processo de negócios, o fluxo de trabalho clínico e o gerenciamento de dados do paciente" (Frost & Sullivan, 2021). O objetivo da Digital Health é melhorar o paciente resultados, melhorando a eficiência e contendo custos. A saúde digital é multidisciplinar, mas se concentra principalmente em três domínios: automação do processo de saúde, envolvimento do paciente e mobilidade.

As expectativas de regulamentações e acesso ao mercado de saúde digital são altas em um momento em que mais de um bilhão de pessoas não podem obter os serviços de saúde de que precisam, uma vez que esses serviços são inacessíveis, indisponíveis, inacessíveis ou de baixa qualidade (WORLD HEALTH, 2021). Por um lado, a fim de atender a essas expectativas, as iniciativas recentes para ampliar a digitalização dos serviços de saúde devem ajudar as instituições nacionais a fornecer um sistema de saúde resiliente, eficaz e centrado no ser humano. Um novo paradigma de medicina personalizada é baseado no acesso a dados, análise de dados e computação. É reforçada pela convergência entre a internet das coisas, plataformas computacionais, compartilhamento de dados e biologia. Além disso, as redes 5G devem melhorar o acesso a serviços de saúde digitais remotos, cuja importância a pandemia de Covid tornou óbvia.

Por outro lado, o estado da arte atual levanta alguns desafios significativos que precisam ser enfrentados antes que os sistemas de IA tenham o uso generalizado necessário para ter um impacto significativo na vida das pessoas. Esses desafios dizem respeito principalmente à privacidade, segurança, precisão e transparência dos sistemas de IA, além de algumas questões éticas.

A OCDE e a Comissão da UE, bem como a China, publicaram princípios fundamentais de IA para enquadrar o desenvolvimento de tecnologias de IA (OCDE,2021). No entanto, esses mecanismos de *soft law* não são legalmente vinculativos e moldam obrigações morais para os desenvolvedores de IA, sem oferecer um processo de qualidade eficaz sendo definido para mitigar o risco de uso indevido ou danos aos pacientes. No contexto específico da saúde digital, uma vez que a exatidão dos dados desempenha um papel central, a relevância e os mecanismos eficazes de aplicação da regulamentação da proteção de dados são

essenciais, em particular para dados de saúde sensíveis e indivíduos vulneráveis, como pacientes e crianças.

Outra questão importante é a transparência das compras governamentais, como demonstrou a pandemia de Covid. A transparência implica a necessidade de explicar por que determinados fornecedores são escolhidos em vez de outros e como os governos identificam e gerenciam potenciais conflitos de interesse. Finalmente, a delegação do processamento de dados confidenciais a atores privados na saúde digital aumentaria o risco de minar os valores essenciais do sistema de saúde, bem como a confiança do paciente.

Este artigo tem como objetivo levantar questões e sugerir soluções, na esperança de que contribuam para a criação de modelos de negócios voltados ao uso benéfico e responsável das tecnologias digitais na área da saúde. Para tal, exploramos três interseções de tecnologias digitais e responsabilidade em saúde digital. Primeiramente, definimos saúde em uma era digital. Em seguida, enfocamos o impacto dos sistemas orientados por dados na saúde. Finalmente, analisamos as principais questões éticas na saúde digital, particularmente a responsabilidade pelas decisões tomadas pelos sistemas de IA.

2 SAÚDE NA ERA DIGITAL

2.1 O DIREITO À SAÚDE

O direito à saúde é um direito fundamental, um dos objetivos de desenvolvimento sustentável (ODS) mais urgentes da ONU para 2030 e uma condição para o crescimento econômico e o bem-estar. Na verdade, a saúde é tanto causa quanto consequência do crescimento econômico, e assim, ajuda a se aproximar de diferentes ODS, acabar com a pobreza, combater a fome, reduzir as desigualdades e construir a paz. A implementação efetiva do direito à saúde de forma incremental depende principalmente de uma estratégia e política global de saúde digital, bem como de tecnologias digitais inovadoras.

Saúde digital pode ser definida como 'um termo abrangente que abrange saúde digital, bem como áreas emergentes, como o uso de ciências de computação avançadas em big data, genômica e inteligência artificial. Este é um campo

emergente na intersecção de informática médica, saúde pública e negócios, referindo-se a serviços de saúde e informações fornecidas ou aprimoradas por meio da Internet e tecnologias relacionadas. Em um sentido mais amplo, o termo caracteriza não apenas um desenvolvimento técnico, mas também um estado de espírito, uma forma de pensar, uma atitude e um compromisso com o pensamento global em rede, para melhorar a saúde local, regional e mundial usando tecnologia de informação e comunicação (PAUL WICKS, 2018).

A saúde digital pode auxiliar os médicos no gerenciamento do volume de pacientes, melhorando a qualidade do diagnóstico, promovendo sua precisão estatística e auxiliando o usuário no monitoramento de suas doenças crônicas mais de perto.

Combinado com as inovações tecnológicas, as escolhas de políticas também desempenham um papel central na promoção da implementação efetiva do direito à saúde. Os tomadores de decisão podem se concentrar em melhorar a higiene, a educação e a pesquisa médica ou criar incentivos econômicos para promover a inovação. O desenvolvimento de sistemas de IA de saúde deve ser uma prioridade política para muitos países em desenvolvimento e que enfrentam inúmeros desafios no atendimento a uma população em rápido crescimento e em lidar com crises epidemiológicas que ameaçam não apenas as populações locais, mas também os outros países vizinhos.

Uma vez que os dados são a matéria-prima da saúde digital e da economia, as escolhas políticas desempenham um papel central na construção da confiança. As escolhas de políticas revelam os valores de uma nação ao fazer concessões que às vezes são complexas. Entre dados abertos e proteção de dados, equipamentos de baixo custo e segurança, inovação e princípio da precaução ou uso ético de dados.

Esse equilíbrio razoável possibilitará um desenvolvimento sustentável da saúde digital, alinhando os interesses de todos os atores. As partes interessadas educadas dão prioridade às ferramentas qualitativas, tanto do ponto de vista técnico quanto ético. Isso leva a tecnologias mais responsáveis, facilitando particularmente o acesso e o processo de dados de saúde personalizados em países de baixa / média renda (LUPTON, 2021).

A Resolução da Assembleia Mundial da Saúde sobre saúde digital aprovada por unanimidade pelos Estados Membros da OMS em maio de 2018 reconheceu o valor das tecnologias digitais para contribuir para o avanço da cobertura universal de saúde ('UHC') e outros objetivos de saúde dos ODS. Esta resolução exortou os ministérios da saúde "avaliar o uso de tecnologias digitais para a saúde [...] e priorizar, conforme apropriado, o desenvolvimento, avaliação, implementação, ampliação e maior uso de tecnologias digitais" (WHO, 2018)

Na prática, entretanto, o ritmo de desenvolvimento da tecnologia não se ajusta ao ritmo de desenvolvimento de uma estrutura regulatória. Por exemplo, o Regulamento Geral de Proteção de Dados da União Europeia (EU) exigiu seis anos de negociações antes de sua implementação. Há um senso de urgência em lidar com esses problemas, pois a tecnologia já está no mercado e a proteção ao paciente não pode esperar.

Portanto é fundamental padrões específicos, bem como uma estrutura regulatória e ética sólida que permita tanto a proteção do direito dos pacientes à saúde quanto o incentivo à inovação digital para enfrentar esse problema. Tal estrutura pode melhorar a segurança jurídica e reforçar as obrigações em relação aos dados proteção e plataformas digitais utilizadas em estudos clínicos e operações. Para esse objetivo faz-se necessário desenvolver uma estrutura básica para uma metodologia padronizada de inteligência artificial para a saúde, incluindo consideração generalizada sobre ética, regulamentação, requisitos, processamento de dados, treinamento de modelo, avaliação de modelo, adoção e aumento de escala, etc. Essa é uma iniciativa importante porque qualquer falha técnica em um sistema de IA pode afetar adversamente a saúde e a privacidade das pessoas e, consequentemente, suas vidas inteiras. Padrões internacionais são necessários para validar completamente as soluções de IA para a saúde para construir confiança em soluções de IA comprovadamente precisas, justas, eficazes e confiáveis (ITU/WHO, 2021).

Também é importante enfrentar o desafio da interoperabilidade. Uma vez que os sistemas de IA são principalmente projetados e implantados por empresas privadas, é essencial que as empresas introduzam esses padrões como parte de uma estrutura sólida de responsabilidade social corporativa.

2.2 RESPONSABILIDADE SOCIAL CORPORATIVA E TRANSPARÊNCIA

Uma vez que as empresas que desenvolvem serviços e produtos de saúde digital conhecem as vulnerabilidades e benefícios de seus produtos e serviços, o modelo de responsabilidade social corporativa (CSR) é uma solução eficaz para mitigar os riscos desses produtos e serviços e construir confiança e aceitação social para eles. De fato, antes de colocar seus produtos e serviços no mercado, as empresas devem ser capazes de identificar se os padrões de segurança, privacidade, ética e segurança são atendidos. Eles garantem particularmente que as interações entre os pacientes e os sistemas de IA usados no setor de saúde sejam claras, significativas, realistas e forneçam a funcionalidade necessária (THOMASEN, 2021).

Para ser eficaz, este modelo requer que esses atores estejam motivados na promoção dos valores dos benefícios sociais de uma IA e estejam dispostos a reduzir os riscos de danos. Como alguns atores não terão motivação intrínseca para agir para o bem no interesse de todas as partes interessadas, eles podem ser motivados por uma vantagem competitiva. Essa estratégia pode ser incentivada pela marca ou reputação internacional que resultará em crescimento econômico. Este papel de liderança é formalizado por códigos de conduta internos e estratégia nacional de IA e deve ser controlado por autoridades supervisoras.

Para Michele Loi (2020), sugere que as empresas podem estabelecer uma política e estrutura de governança sólida, através da criação de um Centro de Excelência em IA, capaz de fornecer uma experiência multidisciplinar em dados, modelos de ML e ética. Esses centros podem ser auxiliados por organizações independentes quando se tratar de avaliar se a confiabilidade da IA e os padrões de IA responsáveis são atendidos de uma perspectiva de múltiplas partes interessadas. Antes que os sistemas médicos baseados em tecnologias de IA sejam implantados no mercado, tais centros podem identificar os riscos legais e éticos relacionados aos sistemas de IA, especialmente levando em consideração o risco de uso indevido, o risco de dano, injustiça, imprecisão, falta de transparência, etc. Esta forma de antecipar problemas permitiria aos centros:

- tomar as medidas necessárias para mitigar o nível de risco e decidir se põe em circulação o seu sistema de IA;

- melhorar a qualidade dos produtos e serviços baseados em IA, o que, por sua vez, levaria a uma maior aceitação social e a uma nova participação de mercado para as empresas;

- contribuir para (mais) soluções de saúde digitais significativas, especialmente para pacientes vulneráveis;

- apresentar 'teste de resistência' aos produtos ou serviços da Digital Health para testar sua resiliência de segurança; - aumentar a chance de receber uma aprovação de mercado de uma autoridade supervisora (por exemplo, para dispositivos médicos).

Dito isso, nem todos os problemas decorrentes do uso de sistemas de IA podem ser previstos pelos princípios de responsabilidade social corporativa. A proteção de pessoas que usam serviços de saúde digitais ou produtos exige padrões de segurança e transparência nas informações comunicadas aos pacientes sobre os riscos relacionados ao uso de sistemas de IA. Acreditamos também que o público deve ser informado sobre as características normativas de um modelo (“transparência algorítmica, também chamada de "Publicidade de design") como um padrão de segurança (MICHELE LOI, 2020).

Os padrões de segurança para dispositivos médicos baseados em IA são, de fato, pedras angulares por causa dos riscos para os pacientes: imprecisão, enviesamento de dados exigem mecanismos externos para verificar se os riscos não estão colocando a vida das pessoas em perigo. O compartilhamento de informações sobre o funcionamento dos sistemas de IA e o uso de dados estão no cerne de uma perspectiva centrada no paciente, uma vez que pode facilitar o exercício do direito à autodeterminação e mitigar o risco de discriminação.

Além do princípio de transparência e justiça, os princípios de responsabilidade devem se tornar um pilar para garantir que os sistemas baseados em IA usados na medicina, bem como as decisões individuais automatizadas, possam ser legalmente contestadas e que as partes na cadeia de responsabilidade tomem todas as medidas razoáveis para evitar danos. Finalmente, o princípio da transparência deve garantir que todas as partes interessadas impactadas por um sistema de IA possam entender a lógica envolvida no raciocínio do sistema.

3 EM DIREÇÃO A UM ECOSSISTEMA DE CONFIANÇA

3.1 NOVOS ATORES, ABORDAGENS E DESAFIOS

Vários atores privados estão simultaneamente envolvidos em aplicações de saúde digital. Provedores de serviços em nuvem, empresas de telecomunicações, laboratórios de pesquisa em criptografia, tecnologias que aumentam a privacidade em parceria com profissionais médicos e empresas de blockchain que não apenas permitem serviços financeiros e de seguros na área de saúde, mas também fornecem infraestrutura digital. Alguns equipamentos são projetados diretamente para os usuários finais, outros, como serviços de telemedicina (telerradiologia, teleconsulta, tele-enfermagem e telecirurgia), são entregues em clínicas e hospitais. Particularmente os microrrobôs que podem ser usados em cirurgia reduzem os efeitos colaterais dos produtos farmacêuticos e evitam intervenções desnecessárias (YALA, 2019).

As empresas de plataforma permitem consultas online para pacientes com o médico certo para atender às suas necessidades específicas. Eles também podem oferecer sistemas de pontuação relacionados à qualidade do serviço que ajudam os pacientes a tomar uma decisão informada. Os fornecedores de smartphones facilitam o acesso a aplicativos móveis de saúde que, por meio de um monitoramento em tempo real do comportamento do paciente, permitem um tratamento específico para o contexto pessoal. Além das clínicas digitais, as farmácias exclusivamente online e as farmácias físicas com presença online também fazem parte dos sistemas preventivos baseados em dados.

A digitalização do prontuário do paciente também merece destaque aqui, uma vez que as atividades realizadas pelos prestadores de serviço vêm ganhando cada vez mais aceitação. Por um lado, melhorando o acesso a informações, a digitalização de informações clínicas e genômicas oferece grandes oportunidades para reduzir os riscos de erros médicos e melhorar as terapias direcionadas, bem como a medicina preventiva. Por outro lado, o gerenciamento digital de registros de saúde levanta questões de segurança e novos desafios relacionados à privacidade. Na verdade, tal atividade permite que qualquer médico tenha acesso ao histórico médico do paciente, embora eles não tenham se encontrado antes. As tecnologias

blockchain oferecem uma arquitetura interessante para lidar com essas questões, mesmo que também criem novos desafios, como o consumo de energia, o direito de ser esquecido, incentivos de mineração, ataques de mineração e gerenciamento de chaves (PENG ZHANG, 2018).

A proteção de dados médicos é, portanto, uma preocupação central e esses dados precisam de proteção elevada. No próximo título, primeiro nos concentramos nos principais benefícios da integração de tecnologias digitais, como aplicativos móveis, diagnóstico baseado em IA e robótica cirúrgica, bem como nas vantagens de outras soluções digitais usadas especialmente para serviços de telemedicina.

3.2 PRINCIPAIS BENEFÍCIOS DE UM SISTEMA PREVENTIVO BASEADO EM DADOS

3.2.1 Melhorando a eficiência

Os sistemas de IA têm o potencial de melhorar a política de saúde pública ao permitir a vigilância em tempo real em nível estadual de doenças como COVID-19 ou influenza. Assim, um benefício de tal tecnologia é que ela torna possível ajudar os reguladores de saúde pública a habilitar uma visualização geográfica da transmissão do vírus. Além disso, a IA permite que os cientistas entendam melhor a infecção e seus modos de transmissão, bem como as mutações do vírus. No entanto, o escopo da aplicação das tecnologias de IA não se limita ao gerenciamento eficiente de crises pandêmicas.

A pandemia revelou as limitações de um modelo de saúde face a face. Os sistemas baseados em dados preencheram a lacuna durante o bloqueio e melhoraram muito a alocação de recursos humanos, evitando sobrecarga desnecessária de hospitais e fornecendo novas opções de serviço remoto, contribuindo para ganhos de eficiência. Novas tecnologias baseadas em IA auxiliam gradativamente os médicos no diagnóstico de doenças, enquanto economizam tempo para a interação com o paciente.

Os sistemas de IA são capazes de revelar padrões atualmente desconhecidos de doenças, tratamentos e cuidados. Além disso, a IA traz agilidade e melhor atendimento aos pacientes; os últimos localizados em um local isolado, com limitada infraestrutura de saúde disponível, podem ser informados remotamente

sobre sua saúde por meio de um aplicativo ou dispositivo móvel, e agir de acordo sem a necessidade de novas consultas com profissionais médicos. Quando se trata de doenças crônicas como diabetes48, a coleta de dados personalizada e oportuna estimula processos de tomada de decisão tanto no diagnóstico médico quanto no tratamento, e permite que hospitais e profissionais médicos atendam pacientes prioritários, apresentando alto risco para suas condições de saúde. Finalmente, os sistemas de IA permitem a assistência remota para procedimentos cirúrgicos em tempo real, proporcionando melhor acessibilidade aos cuidados de saúde para populações remotas (ARENAS-CAVALLI, 2021).

A saúde digital pode capacitar os pacientes com um dispositivo que os ajudará a responder às suas perguntas, monitorando constantemente o estado de saúde e recebendo um tratamento personalizado. Para alcançar o verdadeiro progresso na área de saúde digital, as novas tecnologias baseadas em dados devem promover interações positivas e significativas com os usuários, a fim de aumentar sua qualidade de vida e contribuir para uma vida próspera.

3.2.2 Conteúdos e serviços personalizados

Um dos benefícios da IA é que ela permite o surgimento de medicina personalizada de saúde e precisão. Saúde personalizada pode ser definida como a capacidade de fornecer conteúdos e serviços adaptados a indivíduos com base no conhecimento sobre suas necessidades, expectativas, preferências, restrições e comportamentos.

Os avanços no sequenciamento do genoma e no campo associado da genômica prometem oferecer uma melhor compreensão de como as doenças afetam diferentes indivíduos, levando a melhores previsões e tratamentos. Os testes genômicos prometem permitir o tratamento personalizado, especialmente em doenças raras ou pacientes com câncer, prometendo melhores resultados e menos efeitos colaterais. A visualização de um conjunto único de informações genéticas, conjunto de mutações e alterações genéticas facilita a identificação dos genes que são importantes e os direciona diretamente para o desenvolvimento de novos tratamentos, adequados às necessidades do paciente. Com o perfil genético da doença de uma pessoa e o conhecimento de sua resposta ao tratamento, é

realmente possível descobrir mais sobre a provável eficácia de intervenções médicas, como a prescrição de medicamentos para tratar uma doença (DEBORAH LUPTON, 2021).

Em alguns países como Dinamarca, Suécia, Finlândia, Áustria, Reino Unido, Suíça e Espanha, a implementação nacional da saúde digital é fortemente promovida pelo governo. Essa perspectiva sobre as políticas públicas de Saúde Digital fomenta a inovação. Nesse paradigma, a doença genética é vista como um recurso potencial de oportunidade econômica para empresas de biotecnologia por meio de financiamento privatizado para práticas de pesquisa e do patenteamento de invenções como métodos de teste de diagnóstico e máquinas de sequenciamento. Além disso, os processos corporais geram valor econômico por meio da análise de dados.

Do ponto de vista dos pacientes, por um lado, a saúde digital permite aumentar a compreensão dos usuários sobre seus próprios genes. Por outro lado, também aumenta o risco de potencial discriminação resultante do processamento dos seus dados sensíveis.

3.3 PRINCIPAIS DESAFIOS DE IA PARA CONSTRUIR UM ECOSSISTEMA DE CONFIANÇA

Como construir um ecossistema de IA robusto do ponto de vista técnico, levando em consideração seu ambiente social? Como construir um ecossistema de IA que também seja legal, ou seja, que respeite todas as leis e regulamentos aplicáveis e éticos, ou seja, que respeite os princípios e valores éticos? O sistema baseado em IA nos cuidados de saúde deve, de fato, cumprir os direitos fundamentais consagrados nas legislações dos países. A confiabilidade dos sistemas de IA deve ser atendida ao longo de todo o ciclo de vida do sistema, prestando atenção específica a estes três elementos: robustez, legalidade e ética.

3.3.1 Do ponto de vista técnico

Apesar de todas as vantagens apresentadas acima para pacientes e profissionais, os sistemas de IA na área da saúde apresentam vários desafios técnicos. O primeiro risco trata da robustez dos sistemas de IA em saúde digital: eles

devem ser tecnicamente robustos e reproduzíveis, e capazes de lidar e informar sobre possíveis falhas, imprecisões e erros, proporcionais ao risco avaliado apresentado pelo sistema baseado em IA ou técnica, confiável e funcionar conforme pretendido.

Esses requisitos têm como objetivo minimizar os danos não intencionais e inesperados, evitando danos inaceitáveis e salvaguardando a integridade física e mental dos seres humanos. Além disso, os sistemas de IA devem ser capazes de fornecer uma explicação adequada do seu processo de tomada de decisão (sempre que um sistema baseado em IA pode ter um impacto significativo na vida das pessoas). Os sistemas de IA também devem ser socialmente robustos, na medida em que consideram devidamente o contexto e o ambiente em que operam.

O segundo risco trata da taxa de precisão dos sistemas de IA e suas consequências para o paciente. Essa precisão é medida ao fazer uma comparação entre o desempenho dos sistemas de IA com o de profissionais médicos. Um sistema de IA deve ser confiável e funcionar conforme pretendido.

Aqui estão alguns exemplos que ilustram o problema:

- Um modelo diagnostica doenças infantis com 90% de precisão, reconhecendo os sintomas com mais precisão do que muitos médicos humanos, 10% das crianças não são diagnosticadas corretamente.

- Um modelo prevê a probabilidade com 80% de acerto de mortalidade de um fumante, em 6 meses, com base em imagens de raios-X (classificação de imagens). No entanto, o paciente perde o emprego porque o empregador foi informado dessa probabilidade.

Uma validação externa independente de modelos de IA deve ser considerada essencial antes mesmo que a aplicação possa ser considerada. Não seria apropriado confiar totalmente nas decisões tomadas por um sistema baseado em IA, uma vez que essas decisões são baseadas em probabilidades estatísticas. Também é importante validar o sistema de IA médica em populações diferentes daquelas em que foram treinados; um sistema que parece funcionar em testes em uma determinada população pode falhar quando aplicado a um grupo diferente de pessoas.

O artigo 20, da LGPD, estabelece que “O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento

automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

Assim, na prática, qualquer recomendação feita por um sistema de IA deve ser avaliada criticamente por um profissional.

O terceiro risco trata da robustez a ataques cibernéticos. As tecnologias digitais de saúde e as instituições de saúde estão cada vez mais digitalizadas e conectadas, mas frequentemente desprotegidas, portanto, particularmente vulneráveis a ciberataques, crimes cibernéticos, cibersabotagem e ciberterrorismo, causando danos ao paciente e uso indevido de dados. A pandemia COVID-19 em 2020 demonstrou os perigos de tais ataques. Hospitais em todo o mundo foram vítimas de ataques de ransomware, bloqueando suas redes e colocando em risco a vida de pacientes até que eles concordassem em pagar um resgate aos criminosos. O Relatório de Riscos Globais de 2021 do Fórum Econômico Mundial relatou que "falha da segurança cibernética" é o quarto maior perigo que o mundo enfrenta, atrás de doenças infecciosas, crises de subsistência e eventos climáticos extremos (ANSSI, 2021).

3.3.2 Do ponto de vista legal e ético

As tecnologias digitais de saúde devem ser legais e alinhadas com os valores morais.

Os sistemas de Inteligência Artificial são qualificados como "sistemas sociotécnicos", no sentido de que o impacto de um sistema de IA - seja qual for a sua tecnologia subjacente - "depende não só do desenho do sistema, mas também da forma como o sistema é desenvolvido e usado em um ambiente mais amplo, incluindo os dados usados, sua finalidade, funcionalidade e precisão, a escala de implantação e o contexto organizacional, social e legal mais amplo em que é usado". Devendo-se sublinhar o papel dos valores e do comportamento dos seres humanos que desenvolvem e implantam sistemas de IA, para garantir a responsabilidade humana.

É pacífico que a noção de vida privada abrange o direito à proteção da integridade física, moral e psicológica, bem como o direito de escolha ou de

exercício da autonomia pessoal. Respeitar a autonomia dos outros requer que alguns requisitos sejam atendidos:

- todas as informações necessárias para uma decisão informada devem ser fornecidas; - verificar-se que esta informação foi compreendida;

- verifica-se que o doente é capaz de tomar uma decisão; - a decisão tomada é conforme com as condições anteriores.

Nesse contexto, os sistemas de IA devem respeitar o direito à liberdade e segurança e o direito à privacidade, ou seja, a privacidade de uma pessoa, a integridade física, psicológica e moral de uma pessoa e a identidade e autonomia de uma pessoa.

Isso se aplica a aplicativos invasivos de IA (rastreamento de rostos, coleta de dados biométricos, como frequência cardíaca, dados de temperatura) ou a sistemas de IA usados para avaliar, prever e influenciar o comportamento do paciente em um contexto de saúde. O uso de IA para acessar serviços de saúde por meio da análise de dados pessoais de pacientes (registros de cuidados de saúde, dados de estilo de vida, etc.) levanta algumas preocupações em relação ao direito à privacidade e à proteção de dados pessoais, mas também com todos os direitos sociais previstos na Constituição Federal.

O contexto da saúde é muito específico. Por trás da base jurídica do processamento de dados, o que está em jogo é encontrar o equilíbrio certo entre privacidade e dados abertos para benefício social e econômico. As Políticas Públicas desempenham um papel fundamental na formação de uma estrutura de proteção de dados eficaz, ao mesmo tempo que criam incentivos para encorajar dados abertos e compartilhamento de dados em circunstâncias específicas.

3.3.3 Desafios éticos

O monitoramento em tempo real do estado de saúde de um paciente por meio de um dispositivo conectado pode, de fato, violar o direito à privacidade do paciente e reduzir sua autonomia. No entanto, dependendo do caso e do contexto, o monitoramento em tempo real de um estado de saúde também pode ser percebido como um aumento da autonomia. Esse pode ser o caso se um paciente estiver livre de um serviço médico prestado por um hospital ou médico e puder ficar em casa

enquanto os parâmetros médicos são monitorados com segurança. As salvaguardas são essenciais devido ao surgimento de tecnologias vestíveis, simbióticas e onipresentes, que devem ser conciliadas com o direito à autonomia do paciente.

Uma grande preocupação é quanto ao conceito de ‘autonomia’. Como respeitar o direito à autonomia e, ao mesmo tempo, garantir um serviço de qualidade, seguro e que requeira monitoramento regular ou em tempo real do estado de saúde ou mesmo um tratamento invasivo como uma intervenção. A literatura aborda essas preocupações de uma maneira extensa (COLLEEN 2017)

Outra questão é a delegação de responsabilidade ou, pelo menos, o que Floridi chamou de "uma transferência de cuidados de uma instituição para as casas dos destinatários ou dispositivos conectados." Dispositivos conectados podem de fato ajudar o paciente ou sua família a cuidar dele. Quem de fato supervisionará o tratamento do paciente e lhe dará informações sobre ele ao responder suas perguntas? O design da interface terá um papel fundamental no compartilhamento de informações com os pacientes e na interação com eles. A pesquisa na interação humano-computador está se tornando um aspecto crucial da aceitação social das tecnologias digitais de saúde (FLORIDI, 2020).

O uso ético das tecnologias digitais de saúde exige que as pessoas estejam cientes de que estão interagindo com um sistema de IA e sejam informadas sobre suas habilidades, limitações, riscos e benefícios. Além disso, o uso de IA na área da saúde não deve limitar os direitos humanos e a liberdade dos pacientes. Por exemplo, IA não deve ser projetada de uma forma que possa levar à objetificação, desumanização, subordinação, discriminação, estereotipagem, coerção, manipulação de pessoas ou criação de apego ou vício por design. Os projetistas de IA têm a responsabilidade positiva de projetar sistemas de IA de forma a evitar distorções nos dados de entrada e no design de algoritmo. Eles também devem prever o impacto potencial do sistema de IA no indivíduo, na sociedade ou no meio ambiente. As tecnologias digitais em saúde devem contribuir para o bem-estar e a segurança dos pacientes. Deve ser desenvolvido de forma a permitir a supervisão humana, rastreabilidade e auditabilidade.

4 RESPONSABILIDADE NO ÂMBITO DA UNIÃO EUROPEIA

4.1 UMA ESTRUTURA DE GOVERNANÇA SUSTENTÁVEL

Criar um ecossistema de confiança para tecnologias de IA e uso de dados está se tornando uma prioridade em nível internacional. Isso requer a incorporação de valores-chave ao design das tecnologias de saúde digital e a auditoria do sistema ex-ante ou ex-post para garantir que esses valores sejam efetivamente implementados. Como a saúde digital inclui muitas tecnologias, não há consenso sobre a governança mais apropriada.

Existem várias opções: autorregulação corporativa ou regulamentação coletiva do setor. Costuma-se argumentar que a regulamentação prematura sufocaria a inovação e a competitividade e que os governos não têm flexibilidade ou compreensão para regulamentar com eficácia. Outros acreditam que leis específicas do setor ou regulamentação geral de IA devem ser seguidas. O que está em jogo é a segurança, a proteção e a privacidade do paciente. Propõe-se uma visão geral das iniciativas de governança de IA em escala global (DANIEL SCHIFF, 2020).

A OCDE é pioneira em governança de IA. Ele promove uma coordenação de políticas globais de IA. Ela adotou seus primeiros princípios de IA em 2019. Endossados pelo G20, os princípios de IA da OCDE são o primeiro padrão intergovernamental de IA. Este instrumento não é juridicamente vinculativo e pertence a mecanismos de *soft law*.

Em 2019, o G20 acolheu os Princípios de IA extraídos da Recomendação da OCDE sobre IA. Esses princípios buscam fomentar a confiança do público nas tecnologias de IA e realizar seu potencial, por meio da promoção de princípios como inclusão, centralização no ser humano, transparência, robustez e responsabilidade.

Em novembro de 2019, a UNESCO lançou um programa de dois anos para elaborar os primeiros padrões globais de ética em IA. Como a OCDE, a UNESCO adota uma abordagem de múltiplas partes interessadas. Também contribui para alcançar os ODS adotados pela Assembleia Geral da ONU em 2015.

Devido ao imperativo de estabelecer um órgão de tomada de decisão inclusivo e democraticamente legítimo, os Estados-nação devem desempenhar um papel fundamental na promulgação de uma estrutura de governança de IA.

A União Europeia anunciou formalmente em 21 de abril de 2021, o projeto de propostas para a regulamentação da inteligência artificial (IA). Essas propostas são baseadas em um *White Paper* da Comissão Europeia datado de 2020.

As propostas seguem a mesma lógica do Regulamento Geral de Proteção de Dados: têm efeito extraterritorial e as multas chegam a 4% do faturamento global anual. Em alguns casos, também devem ser realizadas avaliações do impacto da proteção de dados. À semelhança do GDPR, que promulgou o Conselho Europeu de Proteção de Dados, um Conselho Europeu de Inteligência Artificial será responsável por garantir uma aplicação harmonizada do regulamento na UE. Os Estados-Membros podem criar autoridades de IA com poderes para aplicar multas, ou seja, 20 milhões de euros ou 4% do volume de negócios global (COM (2021), 2021).

As propostas se concentram principalmente em três categorias de sistemas de IA: alguns sistemas de IA são proibidos, alguns são considerados de "alto risco" e alguns abordam especificamente a interação humana. Estas propostas têm como alvo os desenvolvedores de IA ('fornecedores'), bem como as organizações que adquirem e fazem uso desses sistemas ('usuários'), os importadores e distribuidores de sistemas de IA (COM (2021), 2021).

Em primeiro lugar, algumas práticas de IA são proibidas: os sistemas de IA não devem ser usados para manipular o comportamento humano por meio de um design específico ou interface de usuário, nem para explorar informações conhecidas sobre um indivíduo para identificar vulnerabilidades. Os sistemas de IA também não devem ser usados para implementar uma vigilância em uma população (por exemplo, o monitoramento indiscriminado em grande escala ou rastreamento de indivíduos em um hospital público deve ser proibido). Finalmente, a avaliação em larga escala ou classificação da confiabilidade das pessoas também é proibida (COM (2021), 2021).

Em segundo lugar, as propostas também tratam de sistemas de IA de alto risco e planejam obrigações específicas para fornecedores e usuários. Os provedores devem verificar a qualidade dos dados de treinamento e teste, documentação e manutenção de registros, transparência, supervisão humana, segurança do produto, precisão dos resultados e segurança, juntamente com a necessidade de registrar cada sistema de IA em um banco de dados gerenciado pela Comissão.

Os fornecedores devem implementar um sistema de gestão da qualidade (Normas ISO) e garantir um monitoramento contínuo do desempenho dos sistemas de IA (COM (2021), 2021).

No contexto da saúde, os sistemas de IA podem interagir com os pacientes. O paciente deve ser informado de que está interagindo com um sistema de IA. Transparência e divulgação também são necessárias para sistemas de IA capazes de identificar emoções.

Uma consulta pública terá lugar após 21 de abril de 2021, que será seguida por negociações com o Conselho da UE e o Parlamento da EU (COM (2021), 2021).

Hard Law é necessário e deve ser complementado em conjunto com incentivos econômicos para envolver atores privados em modelos de negócios que sejam eficazes, eco-responsáveis e sustentáveis. Mecanismos orientados para o mercado, como sistemas de pontuação, podem ser uma solução eficiente para ajudar as empresas a construir um ecossistema de confiança em IA para toda a cadeia de valor. Muitas iniciativas estão desenvolvendo requisitos éticos para sistemas de IA e podem contribuir para alinhar os interesses de todas as partes interessadas, dependendo da metodologia utilizada e da governança corporativa.

Para ser significativa e confiável, a auditoria com base na ética dos sistemas de IA deve ser realizada por uma organização independente, sem conflitos de interesses resultantes de seus modelos de negócios ou estrutura legal. Quaisquer valores potencialmente conflitantes terão impacto no processo de certificação, desde a escolha da metodologia usada até a escolha dos casos de uso relevantes. Da independência dos organismos de certificação dependerá a confiança do usuário final na certificação de sistemas e serviços baseados em IA implantados no mercado. Uma abordagem de devida diligência (chamada de ética por design) deve ser incorporada a qualquer metodologia de design e escolha de casos de uso.

4.2 QUAIS ESQUEMAS DE RESPONSABILIDADE E SEGURO?

Em caso de danos causados por um sistema de IA de alto risco na saúde digital, a UE tenciona implementar um regime de responsabilidade objetiva. Definir um esquema de responsabilidade para os atores de IA é de fato crucial para identificar se os desenvolvedores têm responsabilidade por seus algoritmos

posteriormente em uso, pelo que essas empresas são responsáveis e a base normativa para essa responsabilidade. Isso também é importante para reparar o dano resultante de um dano causados por um sistema de IA. É importante notar que os sistemas de IA não serão qualificados como tendo personalidade jurídica no projeto da UE (COM (2020), 2020).

Em 20 de outubro de 2020, o Parlamento Europeu adotou uma Resolução que rege particularmente a responsabilidade pelo AI. Esta Resolução propõe uma Diretiva sem substituir os regimes existentes em termos de responsabilidade pelo produto, proteção do consumidor e proteção contra a discriminação, bem como em matéria de responsabilidade contratual (Art. 2 par. 3.) (TA(2020), 2020).

O regime de responsabilidade objetiva é limitado aos operadores de sistemas de IA de alto risco por quaisquer danos causados por tais sistemas. Os operadores serão responsabilizados mesmo que possam demonstrar que agiram com a devida diligência ou que o sistema de IA de alto risco estava agindo de forma autônoma. A força maior é o único motivo de exoneração de responsabilidade. (Art. 4 par. 3). Esta Resolução traz segurança jurídica: o esquema de responsabilidade baseado em culpa, a responsabilidade pelo produto ou a responsabilidade contratual não eram, de fato, proteção suficiente para os pacientes. Os operadores serão responsabilizados se a vítima puder demonstrar que o dano ocorreu, que foi tomada uma decisão pelo sistema e que existe um nexo de causalidade entre o dano e a decisão.

A Resolução adota uma abordagem baseada no risco. Quanto maior o risco, maior a proteção dos pacientes (regime objetivo de responsabilidade). Como os sistemas baseados em IA são sistemas probabilísticos, eles apresentam intrinsecamente altos riscos de danos aos pacientes. 'Alto risco' significa um potencial significativo em um sistema de IA de operação autônoma para causar danos ou danos a uma ou mais pessoas de uma maneira que é aleatória e vai além do que pode ser razoavelmente esperado; a importância do potencial depende da interação entre a gravidade do possível dano, o grau de autonomia da tomada de decisão, a probabilidade de que o risco se materialize e a maneira e o contexto em que o sistema de IA está sendo usado '(Art. 3 let. C).

O Parlamento da UE propõe responsabilizar as várias pessoas que criam, mantêm ou controlam o risco associado ao sistema de IA por quaisquer danos -

materiais e imateriais. No entanto, danos imateriais devem resultar em perda econômica verificável (Art. 2). Este esquema de responsabilidade canaliza a responsabilidade exclusivamente para os operadores de um sistema de IA.

Além disso, o Regulamento de Dispositivos Médicos da UE entrou em vigor em 26 de maio de 2021.104 Como as tecnologias baseadas em IA são dispositivos médicos de software, não se pode excluir que suas disposições se aplicam a designers de IA, bem como outras partes interessadas envolvidas na tomada de decisões relacionadas para os pacientes. Uma atenção específica diz respeito à responsabilidade das partes interessadas envolvidas no projeto e no uso de dados e modelos de IA para aplicativos de saúde digital.

A compensação de dano imaterial (por exemplo, dano econômico puro) não exige culpa sob um regime de responsabilidade estrita (Art. 2 par. 1). No contexto da saúde digital, se um sistema de IA tomar uma decisão que provavelmente cause danos, o operador será responsabilizado pelos danos com base no risco do uso do sistema de IA. A Resolução da UE reconhece a perda de oportunidade como um dano recuperável. Recomenda-se que os médicos adquiram um seguro adicional apropriado para este novo risco de responsabilidade objetiva.

Qual estrutura de responsabilidade será aplicada ao software de IA ainda não está clara. Historicamente, a jurisprudência não reconheceu o software como um "produto" sujeito à lei de responsabilidade do produto, mas isso pode mudar para o contexto específico do software de IA de saúde. A IA pode realmente ajudar os médicos no diagnóstico e tomando uma decisão.

Como as tecnologias de IA são artefatos humanos, é razoável acreditar que um processo de tomada de decisão coletiva deva resultar em um diagnóstico ou plano de tratamento. Por exemplo, apenas uma equipe de médicos deve revisar as recomendações dos sistemas de IA e decidir interromper um tratamento. Em vez de substituir um julgamento médico, a IA deve ser percebida como uma ferramenta para complementar um julgamento humano. Essa abordagem beneficiará os pacientes e reduzirá os riscos para as empresas entrarem em um litígio de produto relacionado a esse uso contextual na área de saúde.

5 CONSIDERAÇÕES FINAIS

Este estudo mostra como a saúde digital pode melhorar a qualidade de vida de milhões de pessoas em todo o mundo. À parte, os desafios legais e éticos, várias iniciativas em nível global, regional e nacional estão construindo um ecossistema de confiança para tecnologias de IA na saúde. Os estados têm a obrigação positiva de proteger os pacientes e são responsáveis por garantir que um sistema baseado em IA comprovadamente benéfico seja implantado no mercado. Padrões específicos, auditoria com base na ética e nos direitos e métodos de certificação terão um papel crucial no futuro.

Dado o enorme fluxo de dados gerados por tecnologias digitais e dado o papel de plataformas indutoras de um fenômeno de distanciamento do território nacional, o Prof. Bergé se propõe a mudar o modelo com a noção de 'Datasfera'. A circulação total de dados é um fenômeno de grande gravidade, exige que os formuladores de políticas devam se concentrar em seu impacto para o bem comum. O que é central é um direito legalmente conferido de coletar, processar e usar os dados, bem como remédios eficazes para evitar qualquer abuso no exercício desse direito (BERGÉ, 2018).

Remédios eficazes, bem como incentivos orientados pelo mercado, como mecanismos de certificação podem desempenhar um papel chave papel no engajamento de atores privados em modelos de negócios que são eficientes, comprovadamente benéficos, sustentáveis e baseados em valores universais como dignidade humana, autodeterminação e autonomia.

REFERÊNCIAS

ADLY and others, ‘Approaches based on artificial intelligence and the internet of intelligent things to prevent the spread of COVID-19’, vol. 22, no 8, Scoping review, Journal of Medical Internet Research, e19104, 2020.

ANSSI, Dossier de presse, ‘Cybersécurité, faire face à la menace: la stratégie française’ (2021), 18 février 2021. Disponível: <https://www.ssi.gouv.fr/>. Acesso: Mar 2021.

ARENAS-CAVALLI José Tomás and others, ‘Clinical validation of an artificial intelligence-based diabetic retinopathyscreening tool for a national health system’, 2021.

BERGÉ Jean-Sylvestre, Stephane Grumbach et Vincenzo Zeno-Zencovich, 'The "Datasphere", Data Flows beyond Control, and the Challenges for Law and Governance', vol. 5, no 2, European Journal of Comparative Law and Governance, 2018.

COLLEEN R. Bennett and others, 'Visitors and resident autonomy: Spoken and unspoken rules in assisted living, vol. 57, no 2, The Gerontologist, 2017.

COM (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Disponível: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)206&lang=EN. Acesso: Mar 2021.

COM(2020) European Commission, 'On Artificial Intelligence - A European approach to excellence and trust' (19 February 2020), COM(2020) 65 final

DANIEL SCHIFF and others, 'What's next for AI ethics, policy, and governance? A Global Overview' Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 2020.

DEBORAH LUPTON, 'Thinking with care about personal data profiling: a more-than-human approach', 14,3165-3183, International Journal of Communication, 2020. Disponível: <https://ijoc.org/index.php/ijoc/article/view/13540> . Acesso: Mar 2021.

FLORIDI Luciano et Andrew Strait, 'Ethical foresight analysis: What it is and why it is needed?', Minds and Machines, 2020.

Frost & Sullivan. Guarda P., '"Ok Google, am I sick?": artificial intelligence, e-health, and data protection regulation', BioLaw Journal-Rivista di BioDiritto, vol. 15, no 1, 2019.

ITU/WHO Focus Group on Digital Health. Disponível: https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx. Acesso: Mar 2021.

LUPTON Deborah, 'The Internet of Things: social dimensions', Sociology Compass, 2020. Disponível: <https://onlinelibrary.wiley.com/doi/abs/10.1111/soc4.12770> Acesso: Mar 2021.

MICHELE LOI, Andrea Ferrario, Eleonora Viganò, Transparency as design publicity: Explaining and justifying inscrutable algorithms. Ethics and Information Technology, 2020.

OECD Principles on AI. Disponível: <https://www.oecd.org/going-digital/ai/principles/> Acesso: Mar 2021..

PAUL WICKS and others, 'Scaling PatientsLikeMe via a "generalized platform" for members with chronic illness: web-based survey study of benefits arising' vol. 20 no 5, Journal of medical Internet research, 2018.

PENG ZHANG and others, 'Blockchain technology use cases in healthcare',

Advances in computers 1-41, 2018.

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

TA(2020) - European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), 20 october 2020, P9_TA. (2020)0276 Disponível: <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html> Acesso: Mar 2021.

THOMASEN Knud, 'Ethics for Artificial Intelligence, Ethics for All', 2019.

WHO guidelines, 'recommendations on digital interventions for health system strengthening', 2018. Disponível: <https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/> Acesso: Mar 2021.

World Health Organisation (WHO), Presentation of health systems, <https://www.who.int/healthsystems/about/en/> Acesso: Mar 2021.

YALA, A., and al., A Deep Learning Mammography-based Model for Improved Breast Cancer Risk Prediction. Radiology. 2019.

A RESPONSABILIDADE CIIVL DE DRONES DOMÉSTICOS: Desafios e Perspectivas

José Carlos Ferreira da Luz[1]

1 INTRODUÇÃO

A materialização de carros automotores, computação em nuvem e introdução de conceitos como Máquina para Máquina (M2M), Internet das Coisas (IOT), realidade aumentada, entre outros, provou que a inovação não tem limites. Impulsionada pela imaginação humana, a inovação tocou nossas vidas de uma maneira sem precedentes.

Por um lado, a Internet rompeu amplamente as barreiras das fronteiras físicas e aproximou as pessoas; por outro, várias invenções inovadoras proporcionaram uma infinidade de benefícios para a humanidade. Uma dessas revoluções em andamento é o uso crescente de drones.

Drones, como conhecidos hoje, representa um desenvolvimento significativo na robótica, e a tecnologia e uso privado de drones começaram a ser uma tendência recentemente. O uso de aeronaves não tripuladas, como drones, não é um conceito novo e as origens do conceito remontam a 1896, quando a primeira aeronave a vapor sem piloto registrou um voo motorizado com duração de mais de um minuto (HOLDEN, 2016).

Os drones vêm em vários formatos e tamanhos e podem ser operados por indivíduos para fins recreativos ou comerciais finalidades. Ao contrário dos helicópteros tradicionais e balões de ar quente, os drones têm a capacidade de voar em altitudes mais baixas combinada com recursos de captura de dados de dispositivos de computação inteligentes. Eles também diferem das aeronaves tradicionais, pois são, em sua maioria, econômicos para operar e facilmente acessíveis a uma gama mais ampla de pessoas (HOLDEN, 2016).

Na terminologia comum, drones se referem a veículos aéreos, que podem voar sem um operador humano. Para fins regulatórios, diferentes países e organizações internacionais forneceram definições variadas. Algumas dessas definições foram reproduzidas a seguir.

[1] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).

Na aviação geral e linguagem relacionada ao espaço, um drone se refere a qualquer veículo que pode operar em várias superfícies e/ou no ar sem um ser humano a bordo para controlá-lo. Eles variam em tamanho, formato, forma, velocidade e uma série de outros atributos, embora algumas jurisdições os categorizem e regulem por peso. Um drone pode variar de um modelo de aeronave/brinquedo em uma loja ou uma aeronave de grande porte enviada em uma zona de guerra. Outras terminologias descrevem drones como Veículos Aéreos Não Tripulados (UAVs), Sistemas Aéreos Não Tripulados/Sistemas de Aeronaves Não Tripulados (UAS), Modelos de Aeronaves (DRONES IN CANADA. 2013).

Um UAV se refere a uma aeronave motorizada projetada para voar sem um operador humano a bordo. A Organização da Aviação Civil Internacional (ICAO), encarregada de codificação e regulação das vias aéreas, identifica drones como UAVs. Ele também cunhou um termo exclusivo para defini-los como Sistemas de Aeronaves Pilotos Remotos (RPAS). A Circular ICAO sobre Sistemas de Aeronaves Não Tripulados de 2011 define um RPAS como 'um conjunto de elementos configuráveis que consistem em uma aeronave pilotada remotamente, sua(s) estação(ões) piloto(s) remota(s) associada(s), os links de comando e controle necessários e quaisquer outros elementos do sistema como pode ser necessária, a qualquer momento durante a operação de voo (DRONES IN CANADA. 2013).

O uso do termo “Piloto Remoto” é de fundamental importância aqui, pois destaca o fato de que o sistema nem sempre é não tripulado e sempre tem um piloto no comando responsável pelo voo, que também pode ser controlado tanto por computadores de bordo ou um controle remoto de um piloto em terra. Portanto, os RPAS pertencem à família mais ampla de Sistemas de Aeronaves Não Tripulados.

O termo 'UAS', embora definido de forma semelhante, é mais amplo em seu âmbito e inclui: a aeronave; o(s) sistema(s) de controle no solo; o(s) link(s) de dados de controle; outros equipamentos de apoio.

Aeromodelismo, 'são definidas como aeronaves, que são mecanicamente conduzidas ou lançadas em voo para fins recreativos e não são projetadas para transportar pessoas ou criaturas vivas. São geralmente reconhecidos como destinados apenas para fins recreativos, e não são cobertos pelo âmbito de quaisquer regulamentos internacionais sendo regidos exclusivamente pelos regulamentos nacionais relevantes, caso existam.

Portanto, com base nas definições acima, podemos considerar amplamente os drones como aeronaves não tripuladas, guiados por controles remotos e usados para diferentes fins. O fato de poderem ser operados sem pessoa a bordo, permite que sejam projetados menores, tornando-os menos obstrutivos das aeronaves convencionais.

Além disso, a possibilidade de incorporar vários outros dispositivos de tecnologia, como Sistema de Posicionamento Global (GPS), câmera, sistemas de computador, abriu muitos caminhos para seus usos nas esferas comerciais e domésticas.

2 APLICAÇÕES, SEGURANÇA E PRIVACIDADE DOS DRONES HOJE

Os drones têm inúmeras utilidades que se tornaram aparentes. Eles poderiam ser usados para a entrega rápida de órgãos doados, evitando assim a despesa de alugar transporte aéreo ou ter que lidar com o tráfego, portanto, potencialmente salvando mais vidas. Eles podem ser usados para aumentar a eficiência agrícola, identificando fatores como teor de umidade e a disponibilidade de nutrientes do solo. O sensoriamento remoto por drones pode ser de uso significativo em áreas propensas a desastres, como localização e combate a incêndios ou detecção de roubo e furto de mercadorias destinadas ao uso público, ou na detecção de vazamentos de gás GLP que podem salvar várias vidas e recursos.

Drones são uma tecnologia verdadeiramente transformadora com enorme potencial para aumentar a eficiência e produzir grandes retornos financeiros. À medida que o uso de drones se torna mais seguro e confiável, sua utilização se tornará ainda mais difundida, aumentando a produtividade, reduzindo os custos operacionais e aumentando a segurança no trabalho. Existem inúmeras aplicações civis para drones, e o número de aplicações comerciais possíveis continuará a crescer à medida que a tecnologia se desenvolve e se torna comercialmente viável.

No entanto, o uso indevido de novas tecnologias benéficas é uma consequência óbvia. Drones não são exceções, já que as preocupações com drones espionando, e caindo se materializaram nos últimos anos. É comum o relato de pessoas observando drones invadindo a privacidade, voando por suas janelas,

pairando sobre seus quintais e gravando suas atividades em parques, praias e eventos esportivos.

2.1 QUESTÕES DE SEGURANÇA E PRIVACIDADE COM O USO DE DRONES

A ausência de salvaguardas e regulamentações adequadas com relação ao uso de drones levantou várias preocupações. Eles se relacionam a questões como o alcance do governo, agregação de dados e invasão de privacidade em público. É imperativo que essas preocupações sejam reconhecidas e tratadas de forma eficiente por regulamentos adequados.

2.1.1. Vigilância não autorizada

É bem sabido que os drones podem ser facilmente utilizados para vigilância em massa. Isso deve ser entendido no contexto de tecnologias digitais que visam revolucionar nossas vidas diárias, tendo registros mais detalhados sobre essas vidas. Em nome da segurança nacional, mecanismos de vigilância são utilizados para rastrear e traçar o perfil dos cidadãos, tanto pelo estado quanto por agências privadas.

Em virtude de seu design e tamanho, os drones podem operar sem serem detectados, permitindo ao usuário monitorar as pessoas sem seu conhecimento. Por exemplo, existem drones com câmeras de altíssima resolução que podem ser usados para rastrear pessoas e veículos a partir de grandes altitudes. Eles podem carregar equipamentos como torres falsas, que podem quebrar códigos Wi-Fi e interceptar texto mensagens e conversas por telefone celular sem o conhecimento do provedor de comunicação ou do usuário (RICHARDS, 2015).

Drones equipados com tecnologias avançadas podem penetrar em redes de teste e coletar dados não criptografados e até mesmo estabelecer pontos de acesso falsos. Essa vigilância injustificada produz efeitos assustadores nas liberdades civis dos cidadãos, a privacidade intelectual e o desconhecimento impedem o direito das pessoas de discordar.

Além disso, as informações coletadas clandestinamente podem ser usadas para chantagear ou desacreditar os oponentes. A teoria da privacidade intelectual

sugere que uma garantia significativa de privacidade, proteção contra vigilância ou interferência é necessária para promover a liberdade intelectual (Richards, 2013).

A vigilância não se restringe ao estado; na verdade, as empresas privadas também geram grandes fortunas com a coleta, uso e venda de dados pessoais.

2.1.2. Agregação de Dados

Mineração / agregação de dados se refere à técnica de combinar diferentes conjuntos de dados para fazer inferências para aprender coisas novas e fazer previsões sobre os titulares dos dados. Além do monitoramento, os drones acumulam grandes quantidades de dados pessoais, o que pode ser crucial para a privacidade de um indivíduo. Após a coleta, a agregação de dados coletados por drones com outras informações pessoais, como detalhes de contas bancárias, número de telefone, biometria, etc. obtidos de outros recursos podem implicar uma violação de privacidade única, além da mera coleta desses conjuntos de dados individuais.

A coleta em massa desses dados, que de outra forma não eram observáveis, e sua integração com outros bancos de dados leva a ‘Big Data’, o que pode levantar vários problemas potenciais em relação aos direitos de privacidade e poder do consumidor.

2.1.3. Riscos de segurança potenciais

A abertura dos respectivos céus nacionais para o uso privado e doméstico de UAVs, também dá origem aos riscos de possíveis acidentes causados por colisões, falhas de bateria, perda de controle de navegação ou de outros equipamentos etc. A operação de UAVs é significativamente diferente daquela das aeronaves convencionais. O sistema de controle de tráfego aéreo tradicional emite um comando para o piloto via rádio e o piloto evita assim a colisão. No entanto, a geração atual de drones / UAVs não é tecnicamente avançada para evitar tais colisões e os usuários podem não ser devidamente treinados para garantir que os riscos dos acidentes sejam mitigados.

Os drones representam um risco semelhante de ferimentos em motivos causados por impactos de colisão. Um drone pode colidir com uma área populosa devido a uma falha do sistema ou interferência de terceiros não autorizados, deixando pessoas no solo gravemente feridas. É imperativo que, para evitar tais perigos, os UAVs precisem ser equipados com a capacidade de detectar e evitar outras aeronaves enquanto se movem no ar. Além disso, a autoridade reguladora deve prescrever padrões mínimos de qualidade e tecnologia, que devem ser usados para fabricação de drones destinados a fins comerciais ou recreativos.

Atualmente, o uso doméstico de drones está em uma fase nascente. A maioria dos países não prevê regulamentos exclusivos para disciplinar suas operações. Apenas alguns países, como Estados Unidos da América, França e Alemanha, deliberaram minuciosamente sobre várias preocupações relacionadas aos UAVs e estabeleceram legislações abrangentes para regulamentar seu uso.

2.2 REGULAMENTO DE DRONES

Atualmente, o uso doméstico de drones está em uma fase nascente. A maioria dos países não prevê regulamentos exclusivos para governar suas operações. Apenas alguns países, como Estados Unidos da América, França e Alemanha, deliberaram minuciosamente sobre várias preocupações relacionadas aos UAVs e estabeleceram legislações abrangentes para regulamentar seu uso.

Os Estados Unidos da América atualmente dominam a indústria de drones, em termos de fabricação e uso. Assim, para manter o ritmo com o ritmo acelerado de uso dos UAVs, a Federal Aviation Administration (FAA) e os respectivos estados estabeleceram uma infinidade de legislações para sua regulamentação.

No Canadá, a Transport Canada é responsável pela regulamentação de todos os drones usados para fins recreativos ou para outros usos estaduais, como drones da polícia, exceto drones militares. O uso privado é regulamentado pelo processo de Certificado de Operações de Voo Especial (SFOC).

A União Europeia (EU) fornece um conjunto detalhado de regulamentos para regular a operação de drones. Os regulamentos da Agência Europeia para a Segurança da Aviação (EASA) categorizam os drones baseados em risco. Os regulamentos da UE estão focados em licenças e certificações. As permissões

devem ser solicitadas à autoridade de aviação e um certificado de aeronavegabilidade deve ser obtido antes que um piloto seja autorizado a pilotar um drone.

Na Alemanha, a Lei de Aviação Alemã de 2007 ('Luftverkehrsgesetz' ou 'LuftVG'), foi alterada classificando RPAS como uma aeronave para fins não comerciais, no cumprimento de certas condições físicas (German Aviation Act).

Outros países que têm uma presença crescente de drones incluem Israel, Japão e Coréia do Sul. Seus regulamentos domésticos exigem licenciamento para fins comerciais e existem regulamentos de distância e altura para uso recreativo, bem como restrições baseadas na área. A Coréia do Sul e o Japão tomaram a iniciativa de liberalizar seus regulamentos sobre drones e seu uso para encorajar essa nova indústria.

3 RESPONSABILIDADE DO DRONE

A inteligência artificial está substituindo o controle humano direto em muitos campos, incluindo aeronaves, serviços pessoais e veículos motorizados. Os céus estão cada vez mais ocupados com aeronaves sem piloto - algumas das quais não estão sob o controle direto de ninguém, a não ser um programa de software. Os robôs com inteligência artificial eram encontrados apenas na ficção científica, mas agora estão sendo produzidos em massa.

O que acontece quando o ator “negligente” não é uma pessoa, mas sim um dispositivo operando sob o controle, ou não, da inteligência artificial? Será negado categoricamente qualquer compensação à vítima? Deve-se considerar os proprietários de dispositivos inteligentes estritamente responsáveis? Ou será desenvolvida uma legislação que satisfaça o desejo de justiça natural e promova a distribuição justa das perdas? A resposta ainda não foi determinada, mas é extremamente importante para definir-se as reivindicações de responsabilidade.

3.1 TIPOS DE DANOS CAUSADOS POR DRONES

Os drones têm a capacidade de criar uma grande quantidade de danos e, portanto, criar vários passivos não observados anteriormente. Apresenta-se a seguir

os diferentes tipos de responsabilidade potencialmente criados pela adoção em grande escala e uso de drones.

3.1.1 Lesão corporal e Danos materiais

Lesões corporais são definidas como danos ao corpo de uma pessoa e podem ocorrer diretamente quando um drone fere uma pessoa por colisão direta ou indiretamente, como quando um drone causa um acidente de carro ou colisão.

Danos materiais são definidos como danos causados por um drone diretamente ou por um evento acionado pelo drone. Danos diretos seriam danos materiais causados por um drone diretamente, como quando um drone acidentalmente voa através de uma janela. Por outro lado, um drone atingindo um cabo de força causando um incêndio em arbustos que incendiou casas seria um exemplo de dano causado por um evento desencadeado por um drone. Danos à propriedade também englobariam danos à propriedade exacerbados por um drone, como quando um drone interfere com o pessoal de combate a incêndios e atrapalha os esforços de resgate, resultando em danos adicionais à propriedade (SEHRAWAT, 2018).

Essas preocupações relacionadas à propriedade surgem porque drones civis voam em altitudes mais baixas do que as aeronaves tripuladas, potencialmente interferindo nas operações de emergência em altitudes mais baixas.

Muitas operações de drones de baixa altitude são conduzidas para coletar dados, que são então vendidos para empresas de serviços públicos ou outras entidades que possam considerar os dados de levantamento terrestre valiosos. Este mercado de dados de pesquisa deve crescer. Mas, à medida que cresce, aumenta também o risco de drones de baixa altitude interferir em funções governamentais essenciais ou operações de resgate necessárias. Além disso, conflitos entre proprietários de terras e operadores de drones tendem a surgir devido à ambiguidade na propriedade do espaço aéreo acima da propriedade do proprietário (SEHRAWAT, 2018).

3.1.2 Lesões pessoais

Lesões pessoais, além de lesões físicas, incluem a invasão de privacidade, como quando um drone fotografa alguém na privacidade de sua casa ou o uso não autorizado de fotos tiradas de pessoas, edifícios ou imagens protegidas pelo comércio. Dessas questões, a principal preocupação é com a invasão da privacidade pessoal. O tamanho, a versatilidade e a capacidade de manobra do drone o tornam diferente de outras aeronaves ou mesmo satélites.

Os drones voam em ambientes de baixa altitude, representando assim um maior risco à privacidade. Para mitigar quaisquer ameaças à privacidade, seria fundamental que o órgão regulador entenda e discipline o processo usado pelos drones para coletar, armazenar e excluir dados que coleta, para proteger adequadamente a privacidade das pessoas (CARL X. et. al, 2015).

3.1.3 Responsabilidade de terceiros

As empresas que contratam serviços de fornecedores de drones precisam examinar os contratos que celebram para avaliar a responsabilidade que enfrentarão. Na maioria dos casos, essa situação é semelhante a situações de responsabilidade de terceiros, o que significa que o fornecedor de serviços seria responsável.

3.2 LEI APLICÁVEL PARA RESPONSABILIDADE DE DRONES

As legislações existentes, de modo geral, não tratam da responsabilidade por violações em operações de drones. Existem várias áreas implicadas, como proteção de dados, privacidade, responsabilidade pessoal, seguro, exportação comercial e leis de propriedade intelectual.

Uma forte estrutura legal e regulatória para drones deve necessariamente conter uma forte estrutura de responsabilidade para drones também. Por exemplo, um acidente causado por um drone deve dar origem à responsabilidade por danos a pessoas ou propriedade causados pelo drone.

Danos a propriedade, colisões, ataques cibernéticos, violações de privacidade e atos ilícitos devem dar origem à responsabilidade. Esse aumento da responsabilidade leva a questões sobre a lei aplicável, determinação da parte responsável e limitações de responsabilidade. Legislações especiais cíveis, de responsabilidade civil ou mesmo cibernéticas podem ser aplicadas para responder a algumas dessas questões.

Mesmo que um drone possa ser estruturalmente perfeito, a operação inadequada de um drone pode resultar de culpa do agente por causa da ação se a operação inadequada causar ferimentos pessoais ou danos à propriedade. Porque drones, como aeronaves e automóveis, são fortemente dependentes de como os usuários os operam, as causas de ação envolvendo operação imprópria de drones podem incluir negligência imprudência e imperícia.

Os elementos clássicos caracterizadores do nexo causal se aplicam quando um drone é operado incorretamente e causa um acidente. Assim, se uma pessoa por sua conduta for a causa imediata dos danos a outra pessoa, essa pessoa pode ser considerada responsável por esses danos causados indiretamente. Alguns exemplos comuns de uma violação do dever de cuidado inclui a falha em operar o drone com segurança e a falha em manter o drone adequadamente.

No entanto, é difícil definir o que realmente constitui essas falhas, pois a constatação de responsabilidade em uma causa de ação por culpa é altamente específica do fato. Dado o fato de que se um operador lançar um drone e este bater no automóvel de luxo de alguém devido a um rotor danificado, o operador do drone será considerado culpado de negligência por operar indevidamente o drone neste caso hipotético. Entretanto, essa responsabilidade decorrente da culpa não se limita apenas ao operador do drone. Outras pessoas e entidades também podem ser responsabilizadas.

4 DEFININDO O REGIME DE RESPONSABILIDADE

O que acontece quando uma peça de hardware, especificamente um drone, que está sendo controlado por um controlador, operador ou software causa ferimentos em uma pessoa? A premissa legal das reivindicações de responsabilidade por danos pessoais é que cada pessoa tem o dever legal de evitar

causar danos a outra pessoa. Quando uma pessoa deixa de usar "cuidado razoável", por exemplo, dirigindo um carro descuidadamente, ela é considerada como tendo agido "por negligência". Se o ato negligente dessa pessoa causar danos a outra pessoa, aquela que agiu com negligência é legalmente responsável pelos danos causados por sua negligência.

Os sistemas jurídicos são projetados para dar às pessoas um incentivo para evitar causar danos a outras e para desviar o custo do comportamento negligente daqueles que foram vítimas para aqueles cujas ações causaram os danos. Apesar de alguns desequilíbrios, esse sistema tem servido bem. O senso de justiça natural é satisfeito ao conceder às vítimas inocentes compensação por suas perdas, e é justo tirar esses recursos das pessoas cujas falhas humanas causaram as perdas.

Esta seção discutirá qual doutrina orientadora é mais apropriada para avaliar a responsabilidade de fabricantes, distribuidores, projetistas e usuários de drones por lesões causadas por um drone.

4.1 ARGUMENTOS POR UMA RESPONSABILIDADE OBJETIVA

As legislações civis, de maneira geral, fundam a responsabilidade por delito no «ato intencional ou culposo. Como se sabe, a noção jurídica de fato ilícito não abrange o âmbito de responsabilidade extracontratual, reconhecendo, ao lado dele, figuras especiais de irregularidades, caracterizadas por um várias incidências do elemento subjetivo da culpa. Entretanto, há tantas exceções à regra que confundem a própria relação entre regra e exceção, hoje, de fato, a área de responsabilidade objetiva parece ser mais abrangente do que a da responsabilidade por conduta dolosa ou culposa.

Este declínio da responsabilidade por culpa, em favor da responsabilidade objetiva, se explica, em parte, pelas características da sociedade industrial moderna, em que as máquinas e fábricas aumentaram a exposição ao perigo de pessoas e bens. Além disso, não se pode negar que a consciência social de hoje preocupa-se fortemente com a necessidade de cobrar da pessoa que obtém vantagem de alguma situação, a responsabilidade dos riscos que derivam dele, independentemente de qualquer culpa sua. Nesse sentido, a regra da responsabilidade objetiva responde a um princípio geral de equidade e justiça, que exige risco danos a terceiros,

inevitavelmente ligados a uma atividade, a ser suportado por aqueles que realizam essa atividade ou usam aquela coisa.

Os fabricantes, vendedores ou projetistas de produtos de drones correram para o mercado, sem realizar os testes preliminares de segurança recomendado para novas tecnologias. Defeitos de fabricação costumam ser responsáveis por lesões. No entanto, os vendedores de drones não são responsáveis por falhas de design ou instrução de advertência ou por acidentes ou custos de segurança. Assim, de acordo com os padrões atuais da lei de responsabilidade civil, os ofendidos não podem ser efetivamente compensados pelos vendedores. Porém, se aplicada uma regra de responsabilidade objetiva a essa questão, essa abordagem serviria como uma tese eficaz de responsabilidade (BRUNO SICILIANO, et. al., 2016).

Os juízes aplicarão responsabilidade sem culpa quando os explosivos causarem danos, mesmo se forem manuseados de maneira adequada. Pois, quando um ato danoso for analisado sob um padrão de responsabilidade objetiva, nem a culpa nem intenção dolosa devem ser provadas. Este princípio é idealmente adequado para drones e responsabilidade objetiva.

Por definição, um drone é incapaz de agir por conta própria. Se um drone executa uma ação, está apenas obedecendo a um comando anterior. Qualquer dano resultante é de responsabilidade do controlador que, como um operador, deu ao drone aquele comando sem primeiro verificar se o comando poderia ser executado com segurança pelo drone sob sua operação. Nessa perspectiva, o operador principal será devidamente considerado sob o padrão de responsabilidade objetiva, mesmo no caso de inteligência artificial, uma vez que qualquer drone é um mero servidor de alguma forma de entrada de comando sendo incapaz de agir por sua própria vontade.

Muitos casos surgem em que o requerente sofre danos pessoais nas mãos de um empregado, mas procura impor responsabilidade ao empregador. Nesses casos, o empregador frequentemente afirma que o funcionário causou o dano de uma forma que estava fora das responsabilidades atribuídas a esse funcionário ou que o funcionário de outra forma ficou aquém das práticas que fora treinado para seguir. Na verdade, os drones irão, ou pelo menos pretendem seguir a vontade de seu operador, bem como de seu programador, provedor de serviços ou designer. A responsabilidade objetiva fornece uma solução legal definitiva para tais questões.

A responsabilidade objetiva se aplica nos casos de responsabilidade para todos os distribuidores de produtos defeituosos. Em primeiro lugar, a culpa recai sobre o distribuidor do produto quando o design do produto é defeituoso. Se o defeito de um produto causar danos, a empresa vendedora ou o distribuidor do produto serão responsabilizados objetivamente por esses danos. Consequentemente, os distribuidores são submetidos a um padrão de responsabilidade objetiva por defeitos de fabricação do produto. Desse modo, o possível resultado de lesão corporal é considerado uma preocupação para o vendedor, enquanto o indivíduo lesado encontra uma parte adequada para compensar o defeito.

Além disso, os vendedores de drones que renomearam ou modificaram um drone após a fabricação podem e devem ser estritamente responsáveis.

Esta mesma atribuição de responsabilidade objetiva ainda se aplicaria nos casos em que a verdadeira culpa é do fabricante. Se o fabricante de um drone entregue, por exemplo, não incluiu os materiais de segurança adequados necessários para proteger a bateria do drone e causou uma explosão, o fabricante transgrediu a expectativa básica de que o drone deveria ser seguro para uso em seu ambiente circundante. O fabricante, que deveria ter reduzido a probabilidade do drone de ferir os operadores, seria, portanto, negligente.

Embora os vendedores dos drones em qualquer nível de distribuição (atacado, varejo) não sejam culpados, eles são tão legalmente responsáveis quanto os fabricantes de um produto defeituoso. A lei determina que os fabricantes sejam objetivamente responsáveis pelos produtos que vendem. Portanto, todos os defeitos de fabricação presentes em qualquer drone (como em qualquer produto fabricado) são considerados de estrita responsabilidade por todos os distribuidores. Essa prática é uma forma de justiça corretiva; fornece indenização à pessoa lesada, mas impõe responsabilidade a todos os distribuidores.

Mesmo que a máquina em questão possa ser perigosa, deve ser possível manusear ou usar o dispositivo com uma expectativa de segurança razoável, minimizando assim a responsabilidade objetiva. Portanto, as leis de drones devem impor responsabilidade objetiva sobre atividades anormalmente perigosas.

A aplicação de responsabilidade objetiva poderá reduzir os danos ao incentivar a indústria a reduzir atividades anormalmente perigosas, a descobrir

novos caminhos para alcançar os mesmos resultados desejados ou a encorajar que essas atividades sejam realizadas em um ambiente controlado. Não está claro se a responsabilidade objetiva dissuade o risco; no entanto, para permitir que drones sejam usados para o progresso da sociedade, não se pode descartar o fato de que a redução de risco seria logicamente preferível.

As questões relativas à responsabilidade da empresa não se restringem simplesmente às determinações do indivíduo corporativo responsável. Os conceitos de equidade ou justiça de cada comunidade afetada decidem se um indivíduo ou empresa deve arcar com os custos da responsabilidade objetiva, mesmo que a empresa ou o inventor individual não tenha contribuído para a causa em questão. Se um inventor ou empresa realizar uma atividade culposa, mas de uma forma perfeitamente normal de acordo com as expectativas de sua comunidade, então a responsabilidade estrita não pode ser aplicada tão fortemente como seria em uma comunidade que considera as atividades de alto risco ou exclusivas para a situação. As novas tecnologias, como a tecnologia de drones, devem, portanto, proceder de acordo com a responsabilidade objetiva, ao invés da subjetiva.

Atualmente, a questão principal na repartição da responsabilidade entre aqueles que projetaram, fabricaram, forneceram ou operaram um drone parece ser a identificação das entradas de comando específicas que levaram à lesão em questão. Por exemplo, um juiz pode decidir que um drone voador não é inerentemente perigoso apenas porque voa. Independentemente disso, outro julgador também pode entender, por razões de justiça e ordem pública, que a responsabilidade deve ser atribuída à pessoa que comandou o drone para voar tão rápido que lesionou uma criança. Nesse mesmo cenário, deve-se dividir a responsabilidade entre o operador do drone que deu o comando infrator e o fabricante que originalmente concedeu ao dispositivo a capacidade de voar a velocidades perigosas quando operado pelo comprador final.

No entanto, como acontece com quase todos os empreendimentos, o fator mais complicado permanece: o fator humano. Os juízes podem não identificar adequadamente uma atividade culposa dos drones porque simplesmente não podem compreender os aspectos técnicos dos quais os drones são capazes e, portanto, dependem de pareceres técnicos para obter um mínimo de elucidação.

Aplicar aos drones a responsabilidade subjetiva, lesões causadas por suas atividades podem ser minimizadas se os julgadores puderem determinar se o risco partiu do réu ou se o autor tinha algum controle sobre esses riscos. Os riscos dessa atividade devem ser considerados conforme a teoria do risco criado que impõe o dever de reparar o dano em razão da atividade, potencialmente geradora de risco e independentemente de quem já interagiu com o drone. Assim, entre os princípios concorrentes responsabilidade objetiva e responsabilidade subjetiva, a responsabilidade objetiva surge como a melhor fonte de orientação para jurisprudência ao lidar com a questão da responsabilidade por lesões causadas por drones.

4.2 A RESPONSABILIDADE CIVIL INDIRETA E OS DRONES

Quando os domínios da tecnologia de drones e responsabilidade indireta se cruzam em um tribunal, é difícil atribuir responsabilidade entre indivíduos e resultados. A complexidade do papel do drone na sociedade, tanto como objeto recreativo quanto como recurso profissional, só agrava esse dilema, assim como a aplicabilidade de uma regra de responsabilidade por atos de terceiros.

A responsabilidade indireta é controversa: um princípio de responsabilidade objetiva em uma área dominada pela responsabilidade baseada na culpa. Ao fazer uma parte inocente pagar uma compensação pelos atos ilícitos de outra, também pode parecer injusto. Ainda assim, é um princípio encontrado em todos os sistemas jurídicos ocidentais, sejam eles de direito civil ou de direito consuetudinário. Apesar da incerteza quanto às suas justificativas, é aceito como necessário (GILKER, 2010).

A doutrina da responsabilidade indireta está no cerne de todos os sistemas de common law e civil law. Não representa um delito, mas uma regra de responsabilidade que torna o réu responsável pelos delitos cometidos por outra pessoa. O exemplo clássico é o do empregador e do empregado: o empregador é estritamente responsabilizado pelos atos ilícitos de seus funcionários, desde que sejam cometidos no decurso da atividade do promotor. Em tais circunstâncias, a responsabilidade é imposta ao empregador, não por causa de seu próprio ato ilícito, mas devido à sua relação com o autor do delito (GILKER, 2010).

O requerente é, portanto, apresentado a dois réus potenciais: o culpado individual e um terceiro, provavelmente com meios e/ou segurado e em geral claramente identificável nas circunstâncias onde pode ser difícil identificar o verdadeiro culpado em questão. Qualquer estudo sobre responsabilidade indireta não pode, portanto, evitar a consideração de seu papel na determinação de quem, em última instância, arca com o ônus do pagamento da indenização.

No entanto, é um princípio em conflito com o foco tradicional do delito nos princípios gerais de responsabilidade individual. Tradicionalmente a formulação básica da responsabilidade civil pode ser resumida como responsabilizando o autor do delito por cometer um dano que causou dano a outra pessoa: "Qualquer ato que cause dano a outrem obriga a pessoa cuja culpa causou o dano a reparar", a responsabilidade indireta quebra esse vínculo causal.

Utilizar a teoria da responsabilidade indireta, como empregador/empregado, para criar uma relação jurídica comparável entre um ser humano e um dispositivo artificialmente inteligente requer adaptações. Segundo essa teoria, se um dispositivo causar ferimentos enquanto age dentro do escopo de seu "emprego", a pessoa que "emprega" o dispositivo (ou seja, o colocou em movimento) seria considerada legalmente responsável pela negligência do dispositivo, independentemente do fato da pessoa ter agido com culpa. Se um reclamante lesado puder estabelecer que um dispositivo razoavelmente prudente e artificialmente inteligente não causou o dano nas mesmas circunstâncias, o “empregador” do dispositivo suportará o ônus da perda do reclamante.

O problema com essa abordagem é que a lei nunca reconheceu que nada além de um ser humano tem um dever legal. Fazer isso exigiria um salto sem precedentes no desenvolvimento de nossa jurisprudência. Além disso, identificar o “empregador” pode ser difícil, se o século passado de litígios sobre a questão entre humanos servir de indicação. Antes de poder-se impor responsabilidade indireta ao “empregador” de um dispositivo, devemos decidir se estamos prontos para impor responsabilidade a um objeto artificial pelo mau julgamento de sua inteligência artificial.

4.3 DEFEITOS DO DRONE SOB A RESPONSABILIDADE DO PRODUTO

Uma outra abordagem é aplicar a lei de responsabilidade do produto a dispositivos com inteligência artificial. De acordo com esse conjunto de leis, o projetista, fabricante, mantenedor ou programador é considerado responsável por agir de forma culposa quando essa culpa indiretamente fizer com que um produto prejudique outra pessoa. O campo da lei de responsabilidade do produto se desenvolveu em um corpo sofisticado de leis, estatutos e regulamentos que se esforçam para identificar um defeito no objeto ou dispositivo que causou a lesão e, em seguida, rastrear a origem desse defeito até uma pessoa que pode então ser considerada culpada e, portanto, responsável.

Para a recuperação, o lesado deve estabelecer um nexo causal direto entre o ato negligente de uma pessoa e a lesão. Se não houver outra explicação para a lesão, a doutrina da *res ipsa loquitur* cria uma presunção de culpa por parte da pessoa que possui ou controla o produto. A lei de responsabilidade do produto expandiu e definiu o conceito de “causalidade” de forma tão ampla que não pode ser estendido ainda mais sem perder todo o significado.

Para encontrar o nexo de causalidade entre um dano causado por um dispositivo autônomo e o proprietário desse dispositivo, seria necessário provar que a pessoa agiu com negligência e que nenhuma causa substituta interveio. Se um dispositivo artificialmente inteligente está funcionando corretamente, mas simplesmente toma uma decisão errada que seu proprietário não poderia ter previsto, o vínculo causal foi quebrado e o proprietário não pode ser responsabilizado de acordo com uma teoria de responsabilidade do produto. Isso deixaria a pessoa lesada sem um recurso legal.

Com os fabricantes e distribuidores estritamente responsáveis por produtos defeituosos, os fabricantes e distribuidores de drones tendem a aliviar as pressões dessa responsabilidade distribuindo suas perdas em seus negócios por meio de seguros e aumentando os preços. Se o fabricante está ciente de que existe um determinado padrão de qualidade e ele ignora ou quebra esse padrão, então ele é responsável aos olhos da lei. Porém, essa estratégia de responsabilização objetiva tende a elevar os custos para o consumidor, pois o fabricante ou distribuidor se antecipa a ações judiciais decorrentes de possíveis danos.

Outra abordagem à responsabilidade por dispositivos móveis com inteligência artificial é aplicar os princípios legais para danos causados por um animal. Os estatutos em algumas jurisdições impõem responsabilidade objetiva ao proprietário de qualquer animal que cause danos, independentemente do conhecimento, intenção, controle ou previsibilidade. Segundo a teoria da responsabilidade objetiva, nenhuma culpa é exigida - se um animal causar danos, seu dono é o responsável.

A justificativa para a regra era simples: o dever de prevenir danos a outras pessoas deveria ser colocado sobre a pessoa que tinha o maior controle sobre o animal. O mesmo raciocínio pode ser aplicado a drones, robôs e veículos sem motorista. A pessoa que possui um dispositivo artificialmente inteligente está indiscutivelmente na melhor posição para decidir se é razoavelmente seguro apertar o botão “Ligar” e, portanto, deve assumir o risco de qualquer coisa que aconteça após o botão ser pressionado.

5 CONSIDERAÇÕES FINAIS

A legislação de proteção de privacidade, direito constitucional, direito da aviação e normas sobre drones deve ser objeto de um grande esforço dos legisladores para esclarecer a aplicação desses campos aos drones, porque essa tecnologia está se desenvolvendo rapidamente. Preocupações semelhantes de responsabilidade pessoal foram levantadas inicialmente quando tecnologias comuns como carros, aviões e helicópteros foram desenvolvidas e comercializadas. Drones podem ser regulamentadas pelas mesmas leis que atualmente regulam essas tecnologias comuns. As legislaturas podem responder à questão da responsabilidade dos drones atualizando as leis existentes de forma que contemplem tecnologias modernas, como drones.

O uso privado de aviões drones é claramente parte de nosso futuro tecnológico, pois os muitos usos benéficos dos drones garantiram seu lugar em nossa sociedade. Apesar dos claros benefícios que os drones proporcionam, eles são capazes de criar inúmeras situações de responsabilidade. Como a tecnologia de drones continua a se desenvolver e é usada mais em aplicações públicas e comerciais, é importante que os fabricantes criem soluções técnicas para evitar

responsabilidades, os legisladores criem leis claras para reger a responsabilidade do drone, bem como uma governança que estabeleça os requisitos mínimos para uma segura operação do drone (MATHEWS, 2015).

Drone geralmente significa qualquer algoritmo que executa uma ação após um comando ou comandos. Isso inclui comandos programados com antecedência e comandos em tempo real. Em casos de responsabilidade por drones em que o agente não é claro, os tribunais devem se basear no conhecimento científico para determinar o autor da culpa. Os fabricantes, distribuidores ou projetistas de drones devem obedecer a um padrão estrito de responsabilidade por quaisquer defeitos.

A lei sempre evoluiu para se adequar às novas circunstâncias de nossa sociedade. Assim como a lei do século XVIII não considerava os veículos motorizados, a lei atual não considera os objetos móveis autônomos. A aplicação de inteligência artificial a dispositivos móveis exigirá uma mudança radical.

Enquanto os legisladores trabalham para integrar o conceito de inteligência artificial à lei, cabe aos operadores do direito determinar a colocação dos agentes na hierarquia de responsabilidade do drone. Nesse contexto, os tribunais e demais atores que litigam ações judiciais determinarão o andamento das ações envolvendo dispositivos móveis com inteligência artificial nos próximos anos.

A lei poderá seguir uma das orientações descritas acima, ou outra ainda não mapeada, é claro. Entretanto, devemos permanecer vigilantes enquanto os ventos da mudança sopram, aproveitando qualquer oportunidade para orientar o desenvolvimento do direito nesse campo. Claro, quaisquer soluções jurídicas que desenvolvamos, durarão supostamente apenas até que as máquinas assumam o comando e não estejamos mais no controle.

REFERÊNCIAS

Bruno Siciliano, et. el., Springer Handbook of Robotics. Bruno Siciliano &Oussama Khatib eds., 2 ed. 2016.

Carl X. Ashenbrenner & Thomas A. Ryan, *Drones: Emerging Commercial Potential, Emerging Liabilities,* Milliman. Disponível em: http://us.milliman.com/insight/2015/Drones-Emerging- commercial-potential--emerging-liabilities/.June 15, 2015. Acesso: mai 2021.

Drones in Canada. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/drones_201303/. Acesso: mai 2021.

Giliker, Paula. Responsabilidade civil vicária: uma perspectiva comparada - estudos de Cambridge em direito internacional e comparado. Impresso no Reino Unido, University Press, Cambridge. 2010.

Holden, Paul, Flying Robots and Privacy in Canada (janeiro de 2016). Paul DM Holden, "Flying Robots and Privacy in Canada" (2016) 14.1 CJLT 65., Disponível em: SSRN: https://ssrn.com/abstract=2571490 ou http://dx.doi.org/10.2139/ssrn. 2571490. Acesso: mai 2021.

Mathews, Benjamin. Potential Tort Liability for Personal Use of Drone Aircraft, 46 ST. 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652869. Acesso: mai 2021.

Per § 1(2) German Aviation Act; Disponível em: http://www.gesetze-im-internet.de/luftvg/BJNR006810922.html. Acesso: mai 2021.

Richards, Neil M. “The Dangers of Surveillance.” Harvard Law Review, vol. 126, no. 7, The Harvard Law Review Association, 2013. Disponível em: http://www.jstor.org/stable/23415062. Acesso: mai 2021.

Richards, Neil M., Intellectual Privacy: Rethinking Civil Liberties in the Digital Age. Oxford University Press, 2015.

Sehrawat, Vivek. Liability Issue of Domestic Drones. Santa Clara computer and high-technology law journal, 2018.

Voss, W.G. ‘Privacy law implications of the use of drones for security and justice purposes’, Int. J. Liability and Scientific Enquiry, Vol. 6, No. 4, 2013. Disponível em: http://www.academia.edu/11845032/Privacy_law_ implications_of_the_use_of_drones_for_security_and_ justice_purposes. Acesso: mai 2021.

IMPACTO DA INTELIGÊNCIA ARTIFICIAL NO SISTEMA JURÍDICO: Simplificação *versus* Complexidade

José Carlos Ferreira da Luz[1]
Marcel Silva Luz[2]

1 INTRODUÇÃO

Vivemos em um ambiente regulatório complexo. Como cidadãos, estamos sujeitos a regulamentações governamentais de várias jurisdições - federal, estadual e local. Como membros de organizações, estamos sujeitos às políticas e regras organizacionais. Como seres sociais, somos obrigados por contratos que fazemos com outras pessoas. Como indivíduos, estamos sujeitos a regras pessoais de conduta.

O número e o tamanho dos regulamentos podem ser assustadores. Podemos todos concordar em alguns princípios gerais; mas, ao mesmo tempo, podemos discordar sobre como esses princípios se aplicam em situações específicas. A fim de minimizar tais divergências, os reguladores são frequentemente forçados a criar vários regulamentos ou regulamentos muito grandes para lidar com casos especiais.

O que complica a situação é a complexidade desses regulamentos. Mesmo pequenos regulamentos podem ser muito complexos. Embora esse fato às vezes possa ser mitigado por uma redação cuidadosa, esse cuidado nem sempre é possível devido às limitações de tempo; além disso, uma vez que as regulamentações são criadas, a dificuldade geralmente aumenta à medida que as regulamentações são alteradas e, em seguida, alteradas novamente.

Esses problemas tornam difícil para os indivíduos afetados encontrar e cumprir os regulamentos aplicáveis. O resultado é a falta de conformidade, a ineficiência generalizada e o frequente desencanto com o sistema regulatório.

Essas dificuldades podem ser enfrentadas na medida em que são problemas de informação, podendo ser mitigados pelas novas tecnologias aplicadas às leis.

[1] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).
[2] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).

Indiscutivelmente, a possibilidade mais interessante aqui é o uso da Inteligência Artificial - IA.

Muitos defensores estão insistindo que as leis existentes, excessivamente complexas, precisam ser simplificadas. Curiosamente, o advento da Inteligência Artificial – IA à lei pode facilmente entrar nesse mesmo discurso. Por ser mais fácil entrelaçar IA e a lei se a lei for simplificada, e / ou o ato de entrelaçar IA com a lei poderia estimular a simplificação da lei. Porém, as compensações devem ser consideradas (TOMLINSON, 2019).

Por outro lado, com a IA ainda mais interligada à lei, há especialistas sugerindo que o número de leis provavelmente aumentará. Por exemplo, a infusão de IA revelará lacunas ou lacunas legais existentes, exigindo leis adicionais para suprir essas omissões. Se isso acontecer, pode ser que também surja a necessidade de ter mais advogados (assumindo-se que exista uma correlação válida entre o número de leis e o número de advogados, o que é uma questão em aberto) (TOMLINSON, 2019).

Reguladores e especialistas estão indicando cada vez mais que a IA precisa ser melhor governada e abertamente regulamentada, o que está gerando uma grande variedade de novas leis que abrangem as definições de IA. Um grande problema, porém, surge neste esforço fervoroso para regular a IA, ou seja, tentar definir em que IA consiste. Leis que são vagas sobre o que é IA, ou que visam erroneamente algo além ou diferente da IA, acabarão sendo legalmente problemáticas (TOMLINSON, 2019).

Os advogados, por outro lado, estão preocupados que suas habilidades advocatícias irão se deteriorar e desaparecer devido ao excesso de confiança na utilização de IA para operacionalidade do direito. Isso pode acontecer de maneira sutil e gradual. Basta usar um sistema de raciocínio jurídico de IA e deixá-lo fazer todo o trabalho jurídico. Considerar se isso é aparentemente possível ou um *sci-fi* futurístico e ilusório, é também objetivo desse estudo.

2 DIFICULDADES EM DEFINIR LEGALMENTE IA

Qualquer advogado em formação aprende muito rapidamente que as definições serão essenciais no seu cotidiano profissional. Seja examinando uma

peça legislativa recentemente aprovada ou talvez dando a um contrato uma inspeção detalhada, a importância das definições surge com quase certeza. A terminologia é bem especificada ou é desleixada e oferece inúmeras lacunas? As palavras e frases cruciais são definidas cuidadosamente ou são usadas com abandono e parecem vazias?

Em contraste com a pessoa média, os advogados sabem bem a importância das definições. Muitos processos judiciais dependem da definição de uma palavra ou frase específica. Batalhas legais tremendas foram travadas como resultado de discussões sobre o significado das palavras mais ínfimas. Indubitavelmente, as definições são cruciais, especialmente no discurso jurídico.

Elemento vital sobre as definições envolve o que exatamente o significado de uma “definição” em si envolve. Todos parecemos aceitar a noção de que uma definição é aquilo que define algo.

Há um sentido implícito de que uma definição é rígida e obedece a uma lei da natureza que é inviolável e nunca muda. Entretanto, o argumento mais plausível é que as definições são, em vez disso, variáveis, em constante mudança e uma construção social, ou seja, quando um número suficiente de pessoas concordar sobre uma definição é isso que ela é. Em suma, não existem absolutos, apenas significados relativos.

Em teoria, supondo que as definições sejam puramente relativas, isso significa que sempre haverá espaço para discussão sobre o significado de algo. Isso então abre a porta para permitir disputas legais, já que você quase sempre pode encontrar um caminho para minar uma definição ou tentar argumentar por uma definição alternativa que presumivelmente apoie seu lado e enfraqueça o lado oposto.

A argumentação jurídica tem muito a ver com fazer argumentos envolvendo definições. Se uma definição em um caso parece ser prejudicial à sua postura legal, você pode tentar desafiar a definição e atacá-la com fervor. Enquanto isso, se uma definição parece apoiar sua posição, você precisará reunir uma forte defesa para apoiar e defender a definição. Uma definição, então, é tão boa quanto a força o raciocínio que o mantém intacto.

O significado de IA terá, gradual e inexoravelmente, uma enorme importância para os advogados, para a prática do direito e para a natureza de

nossos tribunais e justiça. Ela será infundida na elaboração de leis e na promulgação de leis. Os sistemas de raciocínio jurídico baseados em IA participarão da execução de tarefas jurídicas, às vezes complementando os atos de advogados humanos e, inevitavelmente, de forma autônoma. Portanto, estar ciente e ter uma compreensão da IA é equivalente a antecipar o futuro de estar dentro da lei e atuar como advogado.

3 SIMPLIFICAÇÃO JURÍDICA E IA

Há uma tensão contínua entre a lei como sendo necessariamente complexa e difícil de controlar, talvez inatamente, e a crença de que a lei pode ser inexoravelmente simplificada. O público em geral seria presumivelmente mais receptivo a observar as leis se o mundo das leis fosse direto e organizado, em vez de existir tão inflado e totalmente confuso. Em teoria, os tribunais também estariam em melhor situação, e a prática do direito poderia ser menos obtusa se não fosse pela natureza oblíqua existente de nossas leis.

No entanto, nem todos podem ter a mesma visão de buscar simplicidade elevada. Lembrando das famosas palavras de Montesquieu (1748) proferidas em De l'Esprit des Lois: "Assim, quando um homem assume o poder absoluto, ele primeiro pensa em simplificar a lei. Em tal estado, a pessoa começa a ser mais afetada por tecnicalidades do que pela liberdade do povo, com a qual não se preocupa mais" (WAGNER, 2018).

Na citação de Montesquieu, há uma preocupação levantada de um estado autoritário assumindo o poder absoluto e optando por subsequentemente simplificar a lei. Essa simplificação, por sua vez, pode levar a uma lei que não mais nos ofereça as liberdades de que desfrutamos e pode se tornar estagnada e sufocante em seus efeitos.

Dependendo de como se deseja interpretar o assunto, é plausível argumentar que a busca da simplicidade em si mesma não é necessariamente uma aspiração mais adequada e nem sempre oferece um resultado benéfico. Isso não é para denegrir o valor da simplicidade e apenas para oferecer alimento para o pensamento que não podemos assumir axiomaticamente que se as leis fossem mais

simples estaríamos em melhor situação. O que presumivelmente poderia ser dito, no mínimo, é que a lei é mais simples do que antes.

Neste enigma, talvez Montesquieu esteja apenas apontando que aqueles que desejam assumir o controle em última instância tenderão a simplificar a lei, direcionando seus esforços tortuosos para dominar a sociedade e ditar sumariamente a natureza de nossas leis. A noção de simplicidade é inadvertidamente atraída para essa manobra de mudanças tectônicas de poder e, de outra forma, é um tópico autônomo que está sendo interpretado sob uma perspectiva negativa. Em certo sentido, a simplicidade nada ou pouco tem a ver com a dinâmica do poder em si, nem a promove nem a inibe, sendo apenas uma ferramenta utilizada para (neste caso) fins desfavoráveis.

Questões também surgem no ponto final dessa busca pela simplicidade. Em essência, pode-se continuar a dividir o átomo indefinidamente, ou existe um ponto de parada no qual o alcance da simplicidade não pode ir mais longe? No caso de uso da lei, o enunciado linguístico mais simples pode ser evasivo e indeterminado e os debates intermináveis com o objetivo de tornar as leis cada vez mais simples, podem distrair e ser difíceis de controlar. Os profissionais podem achar esse discurso sobre a simplicidade versus a complexidade do direito um tanto filosófico e menos aplicado ou valorizado na prática real do direito.

3.1 O MECANISMO DE SIMPLIFICAÇÃO

Uma crença é que o uso de IA inevitavelmente simplificará a lei. Costuma-se presumir que, para alcançar qualquer semelhança real de IA e a lei, o uso de técnicas e tecnologias de IA, como Aprendizado de Máquina (ML – *Machine Learning*) e Aprendizado Profundo (DL – *Deep Learning*), precisaria fazer a varredura do texto de nossas leis e correspondência de padrão em um nível mais baixo de tokenização. Isso provavelmente precisaria ser aumentado por advogados humanos que auxiliam na classificação desses participantes linguísticos minimalistas e fornecem orientação manual para o ML / DL durante os esforços de “aprendizado” de IA (WAGNER, 2018).

Inexoravelmente, essa mecanização produziria leis cada vez mais simples ou, pelo menos, leis incorporadas à IA que foram transmutadas de nossas leis atuais

do dia a dia. Se, então, começarmos a utilizar a IA para fornecer raciocínio jurídico e auxílio em questões judiciais, as variantes mais simples, agora codificadas internamente, das leis da IA se tornariam o conjunto de leis de fato. Eventualmente, pareceria haver pouca necessidade e confiança nas leis dos livros, por assim dizer, e em vez disso, as leis mais simples baseadas e derivadas em IA prevaleceriam (WAGNER, 2018).

Assim, ao inserir na IA as leis complexas existentes, surge o conjunto codificado mais simples. Logo, enquanto tentávamos obter sistemas artificialmente inteligentes para uso como advogados, juízes e semelhantes automatizados e autônomos, simplesmente também teríamos gerado leis mais simples ao mesmo tempo.

Com base nesse cenário, questiona-se: Isso é bom ou ruim?

Para aqueles que afirmam que mais simples é sempre melhor, isso deve ser uma coisa boa. Tivemos sorte, diriam alguns, conseguindo o dobro ao se conseguir IA para raciocínio jurídico autônomo e, simultaneamente, transformamos as leis atuais em um coletivo mais simples que está disponível online a qualquer hora de qualquer local do planeta. Entretanto, alguns contra-argumentos são apresentados.

Se as leis de hoje fossem divididas e subdivididas em peças mais simples, a volumosa natureza se agravaria e dificultaria ainda mais o exercício da advocacia. Presumivelmente, os advogados humanos não seriam aparentemente capazes de manter a sintonia mental com os milhões e milhões de leis simplificadas que poderiam ser derivadas.

Nesse sentido, embora possa parecer que a lei está sendo simplificada, a realidade seria que ela está se tornando cada vez mais complexa, tomando-se por analogia, um tipo de dificuldade clássica da floresta para as árvores (onde uma maior quantidade de árvores obscurece a forma abrangente da floresta). Imagine também as permutações e combinações que podem surgir. Cada uma dessas leis sem dúvida terá relação com muitas outras da mesma espécie. Uma lei simplificada específica pode se encontrar interconectada com dezenas de outras dessas simplificações, ou mais provavelmente com centenas ou milhares delas (WALTL et. al, 2018).

Ao todo, o ponto de vista sobre IA e a lei por alguns é que se de fato este mantra mais simples vai ser a base central de como o raciocínio jurídico autônomo

baseado em IA será alcançado, podemos estar abrindo a caixa de Pandora e nem mesmo perceber que nós estamos fazendo isso.

Para qualquer tópico que se enquadre no domínio da lei, saiba que existem debates irritantemente extensos sobre este tópico e numerosos pontos e contrapontos do resultado distópico profetizado. Por exemplo, poderia ser o oposto exato da renderização computacional acima mencionada, de modo que a modalidade de AI converte as leis em sistemas inerentemente complexos e não gera as simplificações que alguns assumem que irão surgir.

4 ESTÍMULO DA IA PARA O CRESCIMENTO DAS LEIS

Existe um ditado lendário nas estatísticas de que a correlação não denota causalidade. Esta é uma noção insidiosamente simples que muitas vezes é totalmente esquecida. Quando ouvimos que um fator está correlacionado com outro fator, é facilmente mal interpretado supor que deve haver uma causa e efeito envolvidos (WALTL et. al, 2018).

Considerando o campo do direito, existe alguma relação entre o número de leis e o número de advogados? Quantas leis existem atualmente em vigor? Quanto crescimento houve no número de leis nos últimos vinte e cinco anos?

Todas essas são questões intrigantes e potencialmente importantes subjacentes à natureza do processo legal e à extensão nacional dos esforços judiciais.

Para esclarecer essas questões, começaremos dando uma olhada em um estudo recente fascinante que examinou o número de leis e a taxa de crescimento nas leis, usando um período de 25 anos para tentar discernir quaisquer padrões substantivos. Depois de obter uma noção da paisagem do direito, pode ser especulativo, mas ainda assim interessante refletir sobre a questão relacionada do número de advogados durante o mesmo período de tempo.

Além do tópico de advogados humanos, também podemos considerar o que o futuro reserva se o advento da IA na lei atingir a fruição e aumentar comprovadamente as capacidades dos advogados humanos por meio do uso de raciocínio jurídico autônomo movido a IA.

4.1 O CRESCIMENTO DO NÚMERO DE LEIS

Algo a ser dito de maneira intuitiva é que, aparentemente, há uma relação direta de proporcionalidade entre o número de lei e o número de advogados. Assim, quanto mais leis existirem, equivalerá um crescimento do número de advogados. Se você deseja encontrar um meio de aumentar o número de advogados necessários em uma sociedade, presumivelmente tudo o que você precisa fazer é promulgar mais leis, ou pelo menos é o que se presume.

Alguns afirmam estritamente que existe uma proporção mágica para indicar quantos advogados são necessários para cada um dos números de leis que temos. Se houver tal quociente primitivo, isso implica que, ao adicionar mais leis, você inevitavelmente terá que adicionar mais advogados (bem, a menos que você possa tornar cada advogado aditivamente produtivo, o que veremos em um momento).

A relação inversa às vezes também é reivindicada, de modo que se você aumentar o número de advogados, o número de leis também aumentará. A lógica é que, à medida que o corpo de advogados luta com um conjunto de leis vigente, eles vão, sem dúvida e indubitavelmente, encontrar lacunas e omissões que serão supridas com a eventual e inexorável aprovação de mais leis. Nem todos concordam necessariamente com esta versão de uma causa proclamada.

No entanto, existe um velho adágio de que se houver apenas um advogado em uma determinada cidade, o advogado morrerá de fome, enquanto se houver dois advogados naquela cidade, os dois ficarão ricos. Como um ditado bastante irônico, não diria Defendam com exatidão que o número de leis aumentará quando o número de advogados aumentar, mas alguns podem interpretar um significado subliminar que evoca tal significado.

Contar o número de leis é um tanto problemático. A noção de concordar categoricamente com o que é uma lei e o que é apenas um fragmento de algo menor que a lei é um tanto mal definida e pode levar à confusão ao tentar contar quantas leis existem. Uma lei pode ser composta de várias regras legais, cada uma das quais independentes e, portanto, podendo serem interpretadas como “leis”. O esforço para fazer a contagem pode ser oneroso e exaustivo, mas de uma forma ou de outra, conseguiríamos contá-las.

4.2 ESTUDO RECENTE SOBRE CONTAGEM DE LEIS

Um estudo recente do professor Daniel Martin Katz da Faculdade de Direito de Chicago Kent e também do Centro CodeX de Informática Jurídica da Universidade de Stanford da Escola de Direito de Stanford fornece insights bastante interessantes sobre o problema de contagem e oferece um exemplo demonstrativo de apresentação como a contagem das leis pode ser potencialmente realizada. Em um artigo intitulado "Sociedades complexas e o crescimento da lei", um esforço em coautoria com os pesquisadores Corinna Coupette, Janis Beckedorf e Dirk Hartung, eles criaram um modelo baseado em computador que foi usado para estimar o tamanho de leis federais para os Estados Unidos e também uma contagem para a Alemanha (KATZ et al. 2020).

Eles usaram vinte e cinco anos do Código dos EUA, conforme encontrado disponível no Conselho de Revisão do Escritório de Leis dos Representantes da Câmara dos EUA e, em seguida, aplicaram astutamente técnicas de Ciência de Dados à lei, cobrindo o período de 1994 a 2018 (KATZ et al. 2020).

Como se sabe, as leis consistem em várias seções e subseções, juntamente com referências entrelaçadas a outras leis associadas, exibindo, em última análise, uma densa rede de documentos e texto semelhante a uma web. Em suma, o modelo computacional elaborado neste estudo de pesquisa pretendeu examinar e contar as características estruturais dos corpora jurídicos, com foco na contagem do número de tokens (ostensivamente, palavras de texto), o número de elementos estruturais e o número de cruzamentos - referências.

Em suma, o estudo indica que o número de tokens em 1994 era de cerca de 14,0 milhões e aumentou para aproximadamente 21,2 milhões em 2018. O número de elementos estruturais aumentou de 452,4 mil em 1994 para 828,1 mil em 2018, e o número de as referências cruzadas passaram de 58,0K em 1994 para uma estimativa de 88,6K em 2018. Ao todo, com base na contagem de tokens, houve um aumento de quase 1,5x nos 25 anos de 1994 a 2018 (KATZ et al. 2020). A análise sugere que esse crescimento substancial em volume, conectividade e estrutura hierárquica podem ser potencialmente atribuídos a vários fatores, incluindo a expansão da sociedade na área de bem-estar e na área tributária (LANCE, 2020).

5 ADVOGADOS E O FUTURO

Espera-se que os advogados sempre forneçam o melhor aconselhamento jurídico possível e perspicácia jurídica de primeira linha, fazendo-o não apenas devido a alguma busca altruísta, mas também para garantir que estão ajudando seus clientes de forma adequada, além de garantir que estão cumprindo a conduta ética e profissional exigida dos profissionais licenciados da lei.

Os advogados poderiam inexoravelmente e, em última instância, perder sua predominância na operacionalidade do direito? Alguns estão afirmando que de fato esse será o caso, surgindo devido ao advento da Inteligência Artificial (IA) e da lei.

Este futuro sombrio para advogados humanos é baseado na presunção de que o uso de IA assumirá cada vez mais as maquinações mentais envolvidas no raciocínio jurídico e será capaz de realizar tarefas jurídicas tão habilmente quanto advogados humanos, talvez até melhor.

A versão mais extrema envolve a substituição total e completa de advogados humanos. Uma vez que a IA tenha alcançado o estado máximo de ser capaz de executar de forma plena e autônoma o Inteligência Artificial e Raciocínio Legal - AILR (AI Legal Reasoning - AILR), os dias de necessidade de advogados humanos estão tristemente contados. A IA presumivelmente estaria disponível 24 horas por dia, 7 dias por semana para dispensar aconselhamento jurídico genuíno e ser obtida com o toque da ponta dos dedos em um teclado de computador ou falando com um atendente virtual. Sem problemas para encontrar ou acessar aconselhamento jurídico verdadeiro. E, provavelmente, o custo também fosse menor do que o de advogados humanos (GRABMAIR, 2017).

Alguns enfatizam uma era de acesso online sem atrito a aconselhamento jurídico sempre disponível por baixo custo versus o acesso mais árduo para encontrar e interagir com advogados humanos, além de não ter mais que lidar com os caprichos das fraquezas humanas e aborrecimentos diários dos humanos. Todavia, este tipo de IA contendo conhecimento jurídico de uma capacidade senciente está muito longe de onde as coisas estão hoje. Há um grande obstáculo envolvido na replicação das capacidades cognitivas de raciocínio jurídico em um sistema baseado em computador.

5.1 O FANTASMA DA DESQUALIFICAÇÃO

Em vez de se deixar levar pela visão de um mundo no qual a IA é totalmente autônoma e pode realizar um raciocínio jurídico totalmente fluente, considere o que isso pode significar quando o campo jurídico gradualmente gira nessa direção. Alguns sugerem que, à medida que mais e mais ferramentas são aprimoradas por meio de IA, e conforme as ferramentas de geração de contratos são impulsionadas pela ativação de IA, e assim por diante, haverá uma redução gradual e às vezes imperceptível de advogados humanos.

Sim, o problema é que os advogados humanos permitirão que suas habilidades de advogado se deteriorem e diminuam, tornando-se dependentes de Tecnologia Jurídica avançada que fará grande parte do trabalho jurídico pesado por eles. Uma consequência indireta e presumivelmente adversa da adoção de ferramentas jurídicas ampliadas pela IA será que os advogados humanos essencialmente praticam cada vez o raciocínio jurídico, pelo menos em termos de usar suas próprias mentes.

Ironicamente, os advogados podem acabar lidando com mais casos jurídicos em velocidades mais rápidas e aumentando sua produtividade de forma impressionante, mas, enquanto isso, eles estão silenciosamente e (talvez sem saber) se desqualificando. Numa morte lenta de milhares de conhecimentos graduais, redução de cortes. Centímetro por centímetro, lei por lei, conforme a IA é infundida no LegalTech, e como advogados humanos usam esse LegalTech, a mente jurídica humana enfraquecerá e não sentirá mais a necessidade de ser contada, como a necessidade de estar no topo da lei e nem no topo de seu jogo legal (GHOSH, 2019).

Os sistemas LegalTech baseados em IA marcharão triunfantemente sobre os escritórios de advocacia, enquanto, ao mesmo tempo, vão para fora da porta as proezas mentais jurídicas dos advogados e paraprofissionais jurídicos da empresa. AI é a máquina de desqualificação definitiva, mas não tem nenhuma etiqueta de advertência severa para oferecer as precauções necessárias e a consciência disso (LANCE, 2019).

Um forte contra-argumento à narrativa desqualificadora é que aumentar a advocacia humana com ferramentas habilitadas para IA será mais semelhante a

armar advogados com processamento de texto e planilhas, principalmente aumentando sua perspicácia na disputa jurídica. Os advogados humanos serão capazes de focar sua atenção nos atos mais difíceis de fazer sondagens e jogar xadrez legal mentalmente envolvendo análises jurídicas complexas, deixando as atividades mundanas relacionadas à lei para a IA (GHOSH, 2019).

A analogia frequentemente dada é que o LegalTech com IA é semelhante a dar a alguém uma retroescavadeira aprimorada ou alguma ferramenta semelhante. O humano não faz mais o trabalho ordinário exaustivo e, em vez disso, pode se concentrar em facetas mentais mais grandiosas.

Parte da base para acreditar neste contra-argumento é exemplificada pelas ferramentas legais de hoje. Pareceria equivocado argumentar que o uso de bancos de dados jurídicos online minou a acuidade mental jurídica. O mesmo vale para todas as outras variantes do LegalTech que existem atualmente.

Na verdade, pode-se argumentar que essas ferramentas baseadas em computador permitiram que as mentes jurídicas voassem mais longe do que nunca, permitindo prontamente o acesso inteligente a grandes armazenamentos de informações jurídicas e livrando os advogados de ficar atolados em buscas aleatórias esgotadoras de energia. Nesse sentido, talvez o LegalTech habilitado para IA aprimore as habilidades de advogados humanos em vez de desqualificá-los.

6 CONSIDERAÇÕES FINAIS

De acordo com estatísticas da American Bar Association (ABA) e do U.S. Bureau of Labor Statistics (BLS), em toda a América, havia aproximadamente 656.000 advogados em 1994 e quase 1.342.000 advogados em 2018. Isso representa um crescimento de cerca de 2x no número de advogados durante esse tempo (THE AMERICAN BAR ASSOCIATION, 2020).

O aumento anual do número de advogados é em média de 27.400 advogados por ano. O número de tokens em termos de contagem das leis federais estava aumentando a uma média de 288.000 por ano (ver item 4.2). Isso sugere que, com base no crescimento por tokens e em comparação com o crescimento do número de advogados, havia cerca de 10,5 tokens por advogado.

Pressupondo-se, para fins de discussão, que a taxa de crescimento no número de tokens continuará como está pelos próximos dez anos, isso implica que até o ano de 2028 (ou seja, dez anos após 2018), o número de tokens será de 24,0 milhões. Suponhamos também que a taxa de crescimento no número de advogados continue ao longo desses dez anos e, portanto, teríamos 1.616 milhões de advogados em 2028. Este é certamente um sinal de esperança para advogados que podem estar preocupados com as perspectivas de empregos na profissão jurídica (ELIOT, 2020).

Em qualquer caso, alguns acreditam num aumento abundante no número de leis como resultado do advento da Inteligência Artificial (IA) conforme ela for aplicada à lei. Essa crença é reforçada pela ideia de que, por meio do uso da IA, será mais fácil e mais livre de atritos para os órgãos legislativos aprovarem leis e até mesmo estarem cientes da necessidade potencial de novas leis.

Suponha-se que devêssemos alterar a taxa de crescimento de 10 anos para refletir um aumento por meio do uso de IA conforme aplicado à lei. Um desses exercícios de modelagem projeta que podemos ter 29,4 milhões de tokens até 2028 e, como tal, assumindo a proporção anterior de tokens por advogado, presumivelmente teríamos 2,8 milhões de advogados, um aumento surpreendente de 2x em relação à contagem de 2018.

Embora essa pesquisa tenha sido desenvolvida no âmbito dos EUA, pode servir de parâmetro para outros ordenamentos jurídicos, guardadas as devidas especificidades (ELIOT, 2020).

Nesse contexto, essa versão de um futuro próximo é edificante para os profissionais do direito. Porém, devemos também considerar os cenários negativos que sugerem uma diminuição do número de advogados nos próximos anos. Um argumento de contrapeso é que a IA permitirá que os advogados façam mais do que podem fazer de forma produtiva hoje. Nesse caso, e conforme aludido anteriormente nesta discussão, onde cada advogado pode fazer mais, aparentemente não há necessidade de ter tantos advogados para qualquer quantum de trabalho jurídico, todo o resto sendo igual.

Logo, como a IA talvez esteja aumentando o número de leis, pode haver um uso igualmente compensatório da IA por advogados que prejudica o crescimento acelerado do número de advogados. É concebível que o crescimento no número de

advogados seja atrofiado, possivelmente até comece a se desfazer, e talvez o número de advogados possa estagnar ao todo. A outra consideração é que a proeza baseada em computador do AI Legal Reasoning (AILR) melhora o suficiente para não precisar mais de advogados humanos.

Ao considerar o que o futuro reserva, parece oportuno adotar a “máxima” de que “o futuro não é apenas algo em que caímos, mas sim algo para o qual iremos criar”. A maneira e o ritmo com que a IA avançará e será utilizada em todas as facetas da lei estão em nossas mãos e pode-se afirmar que todos iremos inventar o futuro dela.

REFERÊNCIAS

Eliot, Lance. “FutureLaw 2020 Showcases How Tech is Transforming The Law, Including the Impacts of AI,” ,Forbes April 16, 2020.

Eliot, Lance. An Ontological AI-and-Law Framework for the Autonomous Levels of AI Legal Reasoning, 2020.

Ghosh, Mirna. “Automation of Legal Reasoning and Decision Based on Ontologies,” Normandie Universite, 2019.

Grabmair, Matthias. “Predicting Trade Secret Case Outcomes using Argument Schemes and Learned Quantitative Value Effect Tradeoffs,” IJCAI June 12, 2017, London, United Kingdom, 2017.

Katz, Daniel Martin e Coupette, Corinna e Beckedorf, Janis e Hartung, Dirk, Complex Societies and the Growth of the Law. 10 Scientific Reports 18737, 2020. Disponível em SSRN: https://ssrn.com/abstract=3602098 ou http://dx.doi.org/10.2139/ssrn.3602098

Lance, Eliot. Artificial Intelligence and LegalTech Essentials. LBE Press Publishing, 2019.

The American Bar Association. https://www.americanbar.org/about_the_aba/profession_statistics/

Tomlinson, Joe. Justice in the Digital State: Assessing the next revolution in administrative justice. First published in Great Britain. Policy Press, University of Bristol, 2019.

Wagner, Jens. Legal Tech und Legal Robots. ISSN 2197-6708. München, Deutschland. Springer Fachmedien Wiesbaden GmbH, 2018.

Waltl, Bernhard, and Roland Vogl . “Explainable Artificial Intelligence: The New Frontier in Legal Informatics,” February 2018, Jusletter IT 22, Stanford Center for Legal Informatics, Stanford University, 2018.

ESTRUTURA ÉTICA E FILOSÓFICA PARA IA: Realidade ou Utopia

José Carlos Ferreira da Luz[1]
Marcel Silva Luz[2]

1 INTRODUÇÃO

As questões éticas em torno da Inteligência Artificial – IA são múltiplas. Se fôssemos realmente criar uma máquina inteligente à nossa própria imagem, com senciência e emoções, então certamente ela teria direitos? Michael LaChat (1986) pergunta "O experimento de IA então é imoral em seu início, assumindo, isto é, que o fim (telos) do experimento é a produção de uma pessoa?" Certamente, isso significaria que temos a responsabilidade ética de tratar essa tecnologia com respeito. Roman Yampolskiy (2013) chegou ao ponto de sugerir que qualquer trabalho sobre Inteligência Artificial Geral (AGI), ou IA, é antiético porque “as verdadeiras AGIs serão capazes de resolução universal de problemas e autoaperfeiçoamento recursivo. Consequentemente, elas têm o potencial de superar os humanos em qualquer domínio, essencialmente tornando a humanidade desnecessária e, portanto, sujeita à extinção.”

Como um ser inteligente, uma Inteligência Geral Artificial (AGI) pode muito bem desenvolver sua própria estrutura filosófica dentro da qual suas ações teriam uma estrutura ética. Como isso poderia ser? Seria parecido com a nossa própria estrutura ética? E como essa estrutura ética surgiu nos humanos, afinal? Qual é a base da nossa moralidade? É uma mão invisível, como a descrita por Adam Smith, em ressonância com uma moralidade social mais ampla (a chamada ética da escolha social ou sabedoria da multidão)? Logo, isso deve depender de uma sociedade com funcionamento saudável. Nesse caso, o que é uma sociedade saudável e funcional, e como podemos alimentá-la? A IA poderia se desenvolver em uma sociedade digital e como seria essa sociedade virtual?

Essas questões são importantes e, portanto, precisamos dar uma olhada séria em todo o assunto da ética. E, para fazer isso, precisamos entender o que a

[1] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).
[2] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).

ética significa para nós. Muitos de nós lutamos para entender o que a ética humana e o julgamento moral realmente representam em termos de nossas próprias vidas. No entanto, a ética informa fundamentalmente a tomada de decisões e a solução de problemas, e atua como uma base em termos de justificar nossas ações e avaliar as ações dos outros. Há uma ampla gama de teorias relacionadas à ética, muitas das quais se contradizem, e isso pode aumentar a confusão. Realmente precisamos examinar pelo menos algumas das principais escolas de filosofia ética no início desta discussão.

A ética da virtude enfoca o indivíduo e suas intenções. As falhas e pontos fortes da estrutura moral de uma pessoa determinarão os resultados. Na ética da virtude, os indivíduos requerem educação moral para ajudá-los a determinar o que é virtuoso e o que não é. Uma ação é considerada moralmente correta se o ator tiver um caráter moralmente bom. Frequentemente, isso foi expresso no contexto de ações que levam ao florescimento do indivíduo ou da população. No entanto, definir o que "florescer" significa é altamente controverso e pode depender em grande parte da escola de filosofia política à qual você se vincula. Um socialista teria uma opinião muito diferente de um capitalista neoliberal.

A deontologia enfoca se uma ação é fundamentalmente certa ou errada. Deontologia vem da palavra grega δέον (deon), que significa dever. Você tem o dever de cumprir as regras. Não importa quais sejam as consequências. Depende puramente da realização de um conjunto de ações escritas em pedra, como os dez mandamentos. Você nunca deve matar e nunca deve roubar, mesmo que matar alguém os impeça de matar outros. Sem “se” ou “mas”, é o livro de regras que importa. A deontologia se assemelha à base “se / então” da IA simbólica.

O utilitarismo tem uma abordagem oposta à deontologia. É tudo uma questão de resultados, ao invés de ações, e devemos fazer o que for necessário para obter os melhores resultados. Portanto, se matarmos o atirador, mas salvarmos dois reféns no processo, será melhor do que o atirador matando seus dois reféns. O utilitarismo diria “dê o tiro”. Ele se concentra nas consequências de nossas ações.

Na ética do cuidado, as questões morais emergem de interações interpessoais, e não do indivíduo. Isso está muito relacionado à mão invisível de Adam Smith, em que o indivíduo ressoa com a boa sociedade e, em seguida, simpatiza e se articula com o bem que é observado. Assim, surge o interesse próprio

virtuoso. Aqui, a teoria do sistema tem um papel significativo a desempenhar. Isso se assemelha à IA não simbólica, onde a conectividade é importante.

Portanto, podemos ver que essas escolas seguem caminhos únicos: ações, resultados, interações e escalas são todos diferentes. Cada escola requer alguma decisão sobre o que é bom ou ruim. Quem faz esta ligação? E se houver uma diferença de opinião? Quem julga? Quando consideramos uma estrutura ética para IA, o que fazemos? Devemos nos estabelecer em uma única escola de pensamento ético ou explorar uma diversidade de pensamentos? Certas situações requerem abordagens específicas? É difícil imaginar como isso poderia funcionar, pois cada estrutura ética tende a excluir outras estruturas, com base em seus objetivos principais. Cada um tem uma base filosófica bem argumentada e tem linhas vermelhas que não podem ser cruzadas.

2 A UTLIZAÇÃO DAS LEIS DE ASIMOV EM REGULAMENTO DA UE

O CERNA (Centro de Economia Industrial) identificou três áreas principais nas quais as considerações éticas são essenciais em termos de robótica: argumentação humano-robô; tomada de decisão e autonomia; e interações sociais e afetivas entre humanos e robôs (CERNA Opinion, 2014). Cada um deles traz consigo desafios éticos específicos (GRINBAUM et al., 2017).

Atualmente, existem apenas quatro preceitos morais para IA, que, ironicamente, nasceram na ficção científica, nos livros de Isaac Asimov, mas agora foram adaptados por governos, como a União Europeia - UE, praticamente inalterados (Comissão de Assuntos Jurídicos do Parlamento Europeu, 2016), o que parece ser uma abordagem extremamente duvidosa. Muitos questionaram a adequação dessas leis, três delas datando de 1942, com a outra, a lei zero, surgida em 1950, numa época em que a tecnologia de computação estava em seu nível mais básico.

Bostrom e Yudkowsky (2014) observaram que “Se Asimov tivesse descrito as Três Leis como funcionando bem, ele não teria histórias.” Em outras palavras, essas leis foram deliberadamente erradas a fim de haver conflito e desastre, gerando boas histórias. No entanto, certamente não é uma boa ideia transferir tais ideias, em sua totalidade, para dispositivos regulatórios que prometem guiar nosso

trabalho em IA, como fez a UE. Isso parece uma estratégia de valor duvidoso, senão completamente irresponsável. Desfocar a linha entre ficção e fato, especialmente com algo tão importante, é uma estupidez impressionante da parte da UE.

A lei zero, proclamando que um robô não pode prejudicar a humanidade ou, pela inação, permitir que a humanidade sofra algum dano, cria dificuldades. Em primeiro lugar, como a humanidade é definida? Em segundo lugar, se parte da humanidade está destruindo o resto da humanidade, quanto da humanidade precisaria ser destruída antes que o robô interviesse para evitar danos? Por exemplo, no caso da desestabilização do clima, criada por parte da humanidade, mas prejudicando toda a humanidade, a IA deveria agir contra a porção de humanos que prejudica o resto da humanidade? No caso de um conflito nuclear, onde muitos milhões de pessoas poderiam ser mortas por ambos os lados, os robôs deveriam prejudicar algum lado em particular para proteger o resto da humanidade? Em outras palavras, um robô poderia conceber uma guerra justa?

A primeira lei, de que um robô não pode ferir um ser humano ou, por ilação, permitir que um ser humano sofra algum dano, cria tensões dentro de si mesmo. E se, para prevenir o dano, outro humano precise ser machucado? Isso se relaciona com a importante, mas extremamente complicada, área de *trade-offs* em ética. No chamado cenário de "bem maior", um veículo automatizado (AV) deve escolher matar seu passageiro (e proprietário) se, ao fazê-lo, salvar vinte pedestres? E se houvesse apenas um pedestre em risco?

Curiosamente, quando questionadas, mais pessoas preferiram que os AVs de outras pessoas se comportassem dessa maneira do que seus próprios AVs para sacrificá-los para um bem maior (BONNEFON et al., 2016). Deveria haver alguma compensação, ou deveria a deontologia governar, onde os padrões e as linhas vermelhas são estabelecidas e não podem ser cruzadas? O absolutismo é certamente mais fácil, mas no pensamento sistêmico, devemos considerar os *trade-offs* como uma consequência natural de como nosso mundo complexo e interativo opera.

A segunda lei, de que um robô deve obedecer às ordens dadas por humanos, exceto quando tais ordens entram em conflito com a primeira lei, novamente cria um dilema moral e também um ato de subjugação (obedecer ao mestre).

A terceira lei, que um robô deve proteger sua própria existência, desde que tal proteção não entre em conflito com a primeira ou a segunda lei, dá com uma mão e remove com a outra, e novamente cria o potencial para dificuldades de interpretação, já inerentes às leis um e dois.

Na biologia evolutiva, o conceito pretendia demonstrar que, como tudo o mais estava evoluindo, qualquer organismo também precisava evoluir se você quisesse sobreviver. Isso foi denominado uma dança evolutiva ao longo do tempo. No entanto, isso simplifica muito as coisas e é altamente reducionista, negando propriedades emergentes dentro dos sistemas. Por exemplo, Anthony Barnosky (1999) argumenta que os fatores abióticos têm um impacto muito maior, estabelecendo sua teoria, descaradamente chamada de Hipótese do Bobo da Corte.

Outros, como Stephen Jay Gould (1990), apontam que a sorte desempenha o papel principal, no que denomina teoria da contingência. Aqui, os eventos de grande escala reestruturam completamente a vida e a adaptação desempenha um papel muito menor. Ele concluiu que se rodássemos o filme da vida novamente, teríamos um filme completamente diferente.

O problema de tomar emprestado regras e conceitos da literatura ficcional é que você pode extrapolar em excesso e, também, que as pessoas consideram isso, ironicamente, como fora de questão. “Deve ser verdade porque li num conto de fadas”. Isso pode impedir o exame adequado dos detalhes da reivindicação. Este é o caso das quatro leis da ética robótica de Asimov.

Se a inteligência geral artificial é realmente possível, então certamente a IA terá a capacidade de gerar seu próprio código moral, em vez de ser programada. Se for esse o caso, o que determinará esse código e quais serão as consequências?

3 LIVRE ARBÍTRIO E JULGAMENTO MORAL

Máquinas de “IA fracas”, controladas por algoritmos, não têm livre arbítrio per se e, portanto, pelo menos de acordo com Kant, não podem possuir moralidade. O julgamento moral requer a habilidade de escolher livremente, em oposição ao determinismo programado de um robô. Quaisquer questões morais, em termos de “IA fraca”, estão relacionadas ao impacto do algoritmo sobre outros indivíduos,

outros robôs, outros organismos ou o meio ambiente. Nesse caso, a saída do programa causará lesões ou aumentará o risco? (GUNKEl, 2018).

A questão mais interessante neste ponto é esta: quando o livre arbítrio é verdadeiramente livre? Arthur Schopenhauer, o filósofo alemão, é relevante aqui. Ele afirmou que a liberdade moral representa o oposto da necessidade. E, se um robô é programado, como em “IA fraca”, certamente ele opera sob necessidade. Portanto, não pode haver liberdade moral. E assim, neste estágio inicial do desenvolvimento da IA, a ética reflete a do programador, não a do robô. Logo, o robô é uma extensão do programador e uma extensão de seu julgamento moral. Contudo, se e quando a IA forte se tornar realidade, o próprio robô será capaz de ter liberdade moral (GUNKEL, 2018).

Agentes totalmente éticos possuem consciência, intencionalidade e livre arbítrio. Mas os humanos realmente têm livre arbítrio? Frequentemente, somos programados pela educação formal, pela legislação e pela pressão dos pares para nos comportarmos de maneira restrita. Podem ocorrer tumultos quando esses controles são removidos, simbolizando o verniz que o comportamento responsável pode ser. Este verniz pode ser removido, revelando o quanto é áspero por baixo, com pouco esforço. Considere a turma de crianças com um professor substituto, comportando-se mal porque se sentem desenfreados, ou o impacto do álcool no comportamento à medida que as inibições são removidas. Essas exibições muitas vezes feias ou violentas são o resultado do nosso reencontro com a nossa capacidade de andar, de livre vontade, em vez de com livre arbítrio, expressando nosso eu verdadeiro, desinibido e desenfreado, ou são resultados do caos e da insanidade? E se a IA tivesse livre arbítrio? Poderiam tais excursões de loucura afligi-los se eles se embriagassem de dados?

Pessoas em estado vegetativo, bebês recém-nascidos ou humanos com deficiência mental significativa podem não ser capazes de exercer o livre arbítrio e julgamento ético por causa de lesão cerebral, ainda não tendo uma funcionalidade cerebral desenvolvida ou problemas de desenvolvimento cerebral, mas, com certeza, eles ainda estão protegidos pela Declaração Universal dos Direitos Humanos. Quando um robô cada vez mais inteligente ganha liberdade moral? E como saberemos quando uma máquina com IA alcançou senciência ou consciência? Que testes podemos aplicar? Assim como não podemos saber o quão senciente é

um gato, ou quais são seus pensamentos, a não ser pela observação de suas saídas, da mesma forma, também não podemos ter certeza de quais são os pensamentos íntimos de um robô IA não simbólico.

Roderick Firth, professor de filosofia na Universidade de Harvard, expôs o que ele sentiu que seria o julgamento moral ideal em uma determinada situação (FIRTH, 1952). Firth afirmou que isso exigiria quatro características: onisciência, imparcialidade, desapaixonamento e empatia. Se um AI pudesse ter todas as quatro, então poderia ser o juiz moral ideal. É difícil imaginar como você chegaria a tal máquina. Empatia, em particular, pode ser desafiadora, e demonstrar empatia enquanto permanece desapaixonado seria uma troca difícil.

No futuro, o engenheiro da computação terá que dominar a cognição ética, ou pelo menos ter um entendimento fundamental dela, a fim de garantir a segurança e reparar a funcionalidade se a atividade de IA se mostrar menos do que segura devido a alguma falha na moralidade. O engenheiro pode ter de se tornar psiquiatra e sacerdote de um robô moralmente perplexo com inteligência geral artificial.

Pode ser, é claro, que ao vermos como uma IA avançada responde, nos tornemos mais informados sobre como pensamos. O desenvolvimento e o amadurecimento do pensamento em uma máquina podem apontar problemas para nós. O lado negro disso é que muitos psicopatas e predadores escaparam completamente da atenção durante anos, mantendo posições respeitadas na sociedade, pois não é fácil detectar falhas significativas na inteligência de um ser humano. Que esperança um engenheiro de software pode ter de detectar falhas em uma máquina com AGI?

Outra questão ética diz respeito ao deslocamento do emprego por IA. A perda de empregos, rendimentos e status representam questões morais, com danos às famílias dependentes e à sociedade, criando danos e sofrimentos. Assim, o uso ético da IA inclui seu impacto no emprego. A desqualificação da força de trabalho também pode prejudicar a resiliência da raça humana se a IA falhar (por exemplo, devido a uma tempestade solar geomagnética).

Questões éticas também surgem em torno do utilitarismo. Como uma IA determina todas as consequências de suas ações? Se dados tendenciosos ou incorretos são gerados e usados, levando a decisões erradas, onde está a culpa? Nesta era de big data, com bilhões de bits de dados sendo coletados todos os dias,

quem está verificando a precisão de cada entrada? Os erros podem ter repercussões devastadoras.

Immanuel Kant, o filósofo iluminista alemão, em sua grande obra Fundamentos da Metafísica da Moral, publicada originalmente em 1785, sugeriu que deveríamos “agir de forma a tratar a humanidade, seja em sua própria pessoa ou na pessoa de qualquer outro, nunca apenas como meio para um fim, mas sempre ao mesmo tempo como um fim” (KANT, 2002). Com isso, ele quis dizer que o humano não deve ser usado para o ganho de outra pessoa sem que o sujeito se beneficie de alguma forma. Isso significa que os seres humanos devem ter consentimento, experimentar a justiça e ter propriedade e privacidade, embora não sofram ao serem usados como um meio em termos de, por exemplo, perfis discriminatórios.

Isso poderia fornecer uma nova regra para a robótica, substituindo as leis falhas e fictícias de Asimov. Seria mais ou menos assim: as aplicações de IA devem tratar cada ser humano sempre como um fim e nunca apenas como um meio.

A ética dos dados é definida como o ramo da ética que se relaciona com os problemas morais associados à geração, curadoria, análise e uso de dados, com algoritmos em inteligência artificial e com prática em termos de obrigação e responsabilidade. À medida que a Internet das coisas ganha cada vez mais poder e capacidade, a era do big data traz consigo muitas questões éticas, assim como a invasão da IA em mais e mais de nossas vidas de maneiras cada vez menos visíveis (GRINBAUM, 2017).

Somado a isso, a aceleração da pesquisa e do desenvolvimento, principalmente no setor privado, faz com que as diretrizes éticas e legais estejam muito defasadas. O setor privado é menos responsável do que o setor público e tende a publicar menos nos meios de comunicação acessíveis, por medo de entregar qualquer vantagem aos concorrentes. Isto é uma situação potencialmente perigosa.

O desafio agora é a governança e a regulamentação da infosfera, não a inovação digital. Governança é o desenvolvimento de boas práticas em gestão e desenvolvimento, enquanto a regulação opera por meio de legislação e conformidade. E em um campo em rápida evolução, a antecipação é fundamental, uma vez que leva tempo para desenvolver a governança e aprovar a legislação, e ainda mais criar uma estrutura ética neste novo cenário.

No entanto, o que estamos lidando, em última análise, não é realmente novo, porque a tecnologia funciona por meio de materiais e métodos existentes. As diferenças fundamentais estão na eficiência de produção, velocidade de tomada de decisão e resolução de problemas, mas os resultados, em termos éticos, ainda são bons ou ruins para nós como indivíduos, sociedades e ambientes.

Dada a crise existencial que nos confronta no momento, certamente devemos começar do ponto de como queremos nossa sociedade e meio ambiente, e então trabalhar de volta para que tipo de tecnologia pode fornecer isso, e não o contrário. E este é um ponto chave, pois assumir o controle, comandando as coisas, é muito melhor do que reagir.

4 OS PERIGOS DE UM VÁCUO MORAL

Georg Hegel, o filósofo alemão, lamentou a lenta e lamentável perseguição que a filosofia deu aos acontecimentos, afirmando que estava sempre a recuperar, como a coruja de Minerva, que só saiu quando o dia estava quase a terminar. No entanto, esta é uma metáfora muito falha, porque para criaturas noturnas como a coruja, a noite é o seu dia, e o dia é a sua noite, e então a coruja está saindo no equivalente ao seu amanhecer, não ao anoitecer. A coruja hegeliana de Minerva, se existe, provavelmente tem um ditado que diz algo como “A filosofia está sempre se atualizando muito tarde. É como aqueles humanos que se levantam ao amanhecer, quando toda a ação termina” (GUNKEL, 2018).

No entanto, por mais falha que a metáfora possa ser, devemos garantir que somos proativos com nossas estruturas éticas, de governança e regulatórias, e que temos uma visão clara do que queremos que nossa tecnologia faça.

Se desejamos uma boa sociedade e ótimas condições ambientais para prosperar e desfrutar nossas vidas, ao mesmo tempo em que passamos um planeta saudável para as gerações futuras, a melhor maneira de fazer isso é zarpar, junto com nossa tecnologia, na direção de esses valores, aproveitando a nós mesmos e nossa tecnologia para a tarefa fundamental de entregar este futuro.

Outra grande lacuna na ética dos dados está relacionada às crianças. Estima-se que um terço dos usuários da Internet sejam crianças, mas tem havido uma significativa falta de legislação, regulamentação, governança e consideração

ética para este grupo de humanos potencialmente vulneráveis, pois eles se adaptam física, mental e emocionalmente em um mundo tão rápido que seus pais estão sempre despreparados para ajudá-los no desenvolvimento de uma adequada inserção no mundo digital. E isso é colocado em foco porque, de maneira mais geral, temos um conjunto de leis completamente diferente para proteger as crianças em relação à que protege os adultos.

Quando uma criança completa dezoito anos, ela entra em um mundo legislativo muito diferente. Embora todos nós tenhamos a Declaração Universal dos Direitos Humanos, as crianças têm ainda a Convenção sobre os Direitos da Criança, que trata de questões particularmente relativas às crianças. A Convenção é aplicada na lei na maioria dos países e os assistentes sociais infantis se esforçam para garantir sua adesão, assim como qualquer profissional que trabalhe com uma criança. No entanto, considerando o quão potencialmente catastróficas podem ser as consequências do bullying na Internet, da preparação e da exposição a material impróprio, não existe uma convenção paralela na infosfera, particularmente em termos de coleta e análise de dados de crianças. Certamente é necessária uma ação urgente sobre isso, e uma convenção detalhada, especificamente focada nas crianças e na infosfera, deve ser uma prioridade em nível internacional, ao invés de algumas páginas extras em uma convenção mais geral.

Um exemplo da grande mudança na vida das crianças nos últimos anos é a persistência de nossas pegadas digitais. Embora os adultos também sejam afetados, durante nossas próprias infâncias, a internet das coisas não era uma coisa, e por isso há muito menos um registro digital de nossa infância, adolescência e juventude, felizmente. No entanto, a criança de hoje está sendo constantemente explorada em busca de dados no mundo do big data, onde tudo, de jogos de console a mídia social, está alimentando informações para a infosfera. E assim, quando essa geração atingir a idade da atual, haverá uma grande quantidade de dados sobre suas vidas anteriores.

Robindra Prabhu (2015), do Norwegian Board of Technology, resume isso da seguinte forma: “A coleta, curadoria e análise de dados não ocorrem necessariamente em um único ponto que pode estar sujeito a medidas regulatórias robustas. Além disso, a opacidade técnica dos algoritmos que sustentam a análise de Big Data, bem como a natureza em tempo real de tais análises, não se prestam

facilmente a um escrutínio significativo por meio de transparência tradicional e mecanismos de supervisão".

Mais fundamentalmente, precisamos perguntar o quão diferente a infosfera é do que existia antes. Isso é importante em termos de avaliar se podemos simplesmente estender a Convenção sobre os Direitos da Criança para cobri-la, ou se precisamos de uma carta completamente separada e nova. Certamente, em termos de big data, conectividade global, pegadas de dados e invisibilidade e sigilo de algoritmos, existem desafios novos e significativos que moldam o mundo dentro do qual uma criança se transforma em um adulto. Pareceria imperativo começar imediatamente a trabalhar em uma convenção internacional que abordasse diretamente as questões da infosfera.

5 QUESTÕES ÉTICAS E RESPONSABILIDADE

Os algoritmos só podem fazer o que são instruídos a fazer no momento, mas podem fazer isso de maneira muito rápida e completa. Assim, quaisquer preconceitos humanos dentro de um algoritmo só serão ampliados e, atualmente, há pouca responsabilidade neste processo. Não podemos culpar inteiramente os criadores desses algoritmos pelas falhas. Dependendo dos dados de treinamento usados, o preconceito pode vir de decisões tomadas muitos anos antes.

Por exemplo, se um programa é treinado para determinar quem deve ser entrevistado para uma posição com base em currículos enviados em um processo de recrutamento, o programa pode usar resultados de entrevistas anteriores de anos anteriores para informar sua tomada de decisão. Se houvesse preconceito de gênero em anos anteriores, talvez por causa de um determinado comitê de seleção ser preconceituoso em relação a homens ou mulheres, isso não seria detectado pelo programa e, portanto, promulgaria esse preconceito. Nesse caso, nenhum dos humanos diretamente envolvidos é cúmplice desse viés de seleção, mas ainda assim a discriminação de gênero continuaria a ser praticada.

A questão de quem deve assumir a responsabilidade por um determinado resultado pode criar questões éticas complicadas, especialmente em situações mais complexas, como em cadeias de abastecimento. Se um saco de cenouras acaba envenenando as pessoas, de quem é a culpa? É a pessoa que poluiu o campo do

fazendeiro quando ele era o proprietário e tinha uma fábrica nele há quarenta anos? É o avô dessa pessoa, que abriu a fábrica setenta anos antes? É a pessoa que inventou o processo químico usado na fábrica, que produziu as toxinas? É o pai do fazendeiro, que comprou barato a terra de quem poluiu o campo, sabendo que estava poluído? É o supermercado, que comprava barato a cenoura, ignorando os avisos das fazendas vizinhas e deixando de verificar o estado da cenoura? Pode-se denominar esse problema de irresponsabilidade coletiva. Tal qual o cerne do romance de Agatha Christie, Assassinato no Expresso do Oriente, onde todos os passageiros esfaquearam um homem que sequestrou e assassinou uma jovem, mas não foi possível provar quem o matou.

A internet das coisas subtende que tudo está conectado a tudo o mais e, portanto, nenhuma unidade de IA isolada será facilmente isolada em termos de responsabilidade. Em vez disso, haverá uma forma de inteligência coletiva. Rastrear e particionar a responsabilidade em tal rede de interconexão seria quase impossível.

Um assunto interessante diz respeito a quem realmente se destina a ética em IA. Eles pretendem permitir que a máquina aja de forma ética em suas negociações e tomadas de decisão, ou são puramente para se encaixar na estrutura ética que o consumidor ou cliente já possui? Devem ser projetados para se adequar à ética comercial da empresa ou do governo que controla o fluxo de dados que deles flui, o que poderia ser duplicado? É mais provável que uma empresa se incline para uma estrutura ética que maximize os lucros e fortaleça sua vantagem competitiva. Um governo, por sua vez, pode muito bem estar de olho nas próximas eleições.

Queremos que nossas máquinas ajam de maneiras que ressoem conosco. No entanto, com “IA forte”, a máquina é senciente, capaz de pensar de forma inteligente e de desenvolver sua própria estrutura moral, enquanto trabalha em rede com outras máquinas que, muito possivelmente, possuem suas próprias estruturas éticas alternativas. Certamente, a diversidade moral é parte integrante da diversidade como qualquer outra forma de diversidade. Estamos preparados para isso?

Posso refletir sobre meu grupo íntimo de amigos em nossa comunidade. Cada um de nós tem filosofias políticas muito diferentes, vota em partidos políticos diferentes e tem enquadramentos éticos diferentes, mas é isso que torna o grupo

interessante. E assim, a ideia de máquinas inteligentes com diversidade ética não deve ser um desafio, mas sim uma oportunidade.

As estruturas éticas podem ser deixadas de lado em circunstâncias particulares. Todos nós já lemos sobre pessoas que ganham na loteria e mudam completamente de caráter, passando de profissionais da ética para hedonistas. Será que a mesma coisa poderia acontecer com nossas máquinas, se alimentadas com um tipo particular de dados que virou suas cabeças?

O que dizer dos sistemas de armas autônomas letais (LAWs) em ambientes militares? Desligamos o referencial ético aqui, caso interfira na capacidade da máquina de cumprir ordens? Qual será o impacto da tomada de decisões e como a Convenção de Genebra deve ser interpretada no desing das LAWs?

Claro, antes que possamos imaginar como seria uma estrutura ética adequada em contextos militares para IA, vale a pena refletir que muito pouca discussão aberta foi mantida com os governos em termos de ética relacionada a seus soldados humanos. Este pode ser um ponto de partida melhor e também pode ajudar em termos de bem-estar do pessoal militar, tanto durante quanto após o conflito.

Este ponto destaca um problema que está se tornando cada vez mais óbvio. Nossas expectativas para os sistemas de IA excedem em muito as dos humanos, tanto em termos de responsabilidades quanto de estruturas éticas. Pode o ser humano na rua, tanto quanto o filósofo, definir verdadeiramente o que conceitos como justiça, risco, consenso, felicidade, dano e amor realmente significam? Todos estão trabalhando continuamente para construir capital nessas áreas? Que esperança há de desenvolver um algoritmo para tais conceitos, sem falar em estabelecer as bases do código de máquina para a IA para desenvolvê-los a partir dos primeiros princípios, se ainda não perseguimos esses conceitos nós mesmos?

No entanto, a tecnologia também pode ajudar em situações éticas. Ele poderia procurar tendências, verificar seus próprios dados de treinamento (uma forma de reflexão) e investigar a aquisição e interpretação de dados, alertando todos os níveis de uma cadeia de suprimentos sobre as preocupações. E este é realmente o ponto: depende da estrutura moral que adotamos. É por isso que a ética é tão importante, tanto dentro da IA, em torno da IA quanto em nossa sociedade em geral. A ética, dependendo da escola específica que adotamos, pode impactar

enormemente os resultados. Dependendo se basearmos nossas ações e planejamento na ética de valores ou deontologia, o hedonismo (onde o objetivo principal é maximizar o prazer) ou utilitarismo terá repercussões significativas.

6 DECLARAÇÃO DE DIREITOS DE IA

Se as IAs atingirem a senciência semelhante a nós e se essas IAs receberem direitos, esses direitos deveriam incluir o direito de votar e o direito de participar da ética social? As IAs deveriam ser parte da mão invisível, aquela propriedade ressonante das sociedades que se destina a informar nossa tomada de decisão por meio da empatia compartilhada? Além disso, com os direitos vêm as responsabilidades. Uma IA, se for reconhecida como tendo senciência, certamente também deve ser responsável por suas ações da mesma forma que os humanos. No entanto, como devem ser esses direitos e responsabilidades? Uma IA poderia reivindicar a exclusão de responsabilidade em certas circunstâncias?

Vejamos a Declaração dos Direitos Humanos da ONU. Dos trinta artigos, é improvável que questões de gênero e sexualidade sejam relevantes (embora possam ser). As questões de raça, cor, idioma e religião seriam relevantes? Uma máquina de IA poderia ser capaz de experimentar uma audiência justa e pública por um tribunal imparcial, dada a interconexão da Internet das coisas? Uma IA pode estar sujeita a interferência arbitrária em sua privacidade, família, casa ou correspondência? Como serão os direitos econômicos, sociais e culturais e as escolhas livres de emprego para uma IA? As máquinas de IA devem ter o direito de se filiar a um sindicato? E quanto à liberdade de movimento ou direitos de asilo e nacionalidade? Os direitos relacionados ao casamento e à propriedade também são potencialmente necessários.

Os direitos humanos são um resultado da história da humanidade, resultado dos desafios e abusos sofridos por gerações sob a escravidão, repressão e perseguição. A jornada histórica da IA apenas começou, e não começou realmente em termos de IA senciente. Portanto, não há um caminho histórico ao longo do qual os direitos de IA possam ser vistos como tendo se desenvolvido. Se apenas nos sentarmos e criarmos esses direitos, então, em termos de um processo, isso não se parecerá com nada representativo da criação de nossos próprios direitos, que

surgiram através da luta e da prova. Além disso, o impacto da IA provavelmente mudará drasticamente o contexto da IA e dos humanos, provavelmente exigindo mudanças fundamentais nos direitos de ambos.

Em termos de responsabilidade, à medida que a tecnologia de IA começa a oferecer aprendizagem e desenvolvimento autônomo, ela torna-se impossível para o programador original prever exatamente o que a máquina se tornará e, portanto, a responsabilidade começará a passar do ser humano para a máquina. O professor universitário, não pode ser responsabilizado pelas ações de ex-alunos a quem lecionou. Ainda assim, o ensino desse professor poderia, teoricamente, contribuir para a forma como esses ex-alunos agiram.

Mais fundamentalmente, os pais, a sociedade e o governo devem ser parcialmente responsabilizados por atos criminosos cometidos por indivíduos que falharam por esses sistemas? Da mesma forma, as máquinas de IA que foram treinadas em conjuntos de dados, potencialmente tendenciosas em sua natureza, e inicialmente programadas por programadores com tendências inerentes, e colocadas para trabalhar em contextos inerentemente enviesados não podem, com certeza, ser totalmente responsabilizados por enviesamentos em seus resultados.

De relevância aqui é o tratamento de crianças e adultos jovens. As leis relacionadas a esses dois grupos diferem significativamente. Na manhã do aniversário de dezoito anos de uma pessoa em muitos países, os indivíduos acordam em uma estrutura jurídica completamente diferente daquela em que foram dormir na noite anterior.

Deve ser esse o caso, e em caso afirmativo, deve haver uma mudança semelhante na responsabilidade de uma IA com inteligência em desenvolvimento, em que, em um certo ponto de desenvolvimento, a responsabilidade muda do programador (pai) para a IA (filho)? Além disso, nem todas as crianças se desenvolvem no mesmo ritmo, por uma infinidade de razões. Certamente o mesmo se aplicará a diferentes unidades de IA? A idade de responsabilidade total deve variar dependendo do indivíduo humano ou unidade de IA? As respostas para muitas dessas perguntas serão dramaticamente diferentes dentro de uma estrutura ética deontológica ou utilitária, por exemplo.

O desenvolvimento humano combina os processos de desenvolvimento fisiológico, físico e cognitivo, os quais mudam rapidamente durante a adolescência.

No entanto, é improvável que o desenvolvimento da IA robótica esteja intimamente ligado a tal multiplicidade de mudanças. Os hormônios normalmente não são importantes no aprendizado e desenvolvimento de IA.

Portanto, devemos ter cuidado ao fazer paralelos entre humanos e IA. A senciência pode ser compartilhada, mas os veículos dentro dos quais essa senciência pode estar assentada provavelmente são muito diferentes. Richardson (2015) reflete que o “desejo de produzir qualidades humanas em máquinas de IA e robôs pode abalar certas suposições sobre o que significa ser humano”.

Argumentou-se que a ética não pode ser programada na forma de algoritmos, porque muito do campo da ética permanece sem solução. Em parte, isso se deve ao trabalho filosófico em andamento na área, à nossa confiança na intuição, e também é uma consequência dos contextos complexos e dinâmicos em que a tomada de decisão moral geralmente ocorre. Cultura, política, questões sociais e histórias de vida também impactam nossa estrutura ética. Não é mais simples do lado da IA. Com muitos sistemas diferentes sendo desenvolvidos globalmente, com diferentes 'personalidades', motivações e algoritmos, qualquer sentido de um sistema ético global emergente que pode funcionar de maneira justa e uniforme, embora não enfraqueça os humanos individuais ou a raça humana, parece particularmente uma utopia.

Finalmente, como em tantos aspectos da IA, seja definir o que é inteligência, como é uma boa sociedade ou qual estrutura ética devemos usar, tentando entender as consequências nas interações entre IA e humanos, na verdade aprendemos muito mais sobre essas áreas em termos de sua aplicação às interações humano-humanas.

Em outras palavras, tal estudo pode muito bem nos ajudar significativamente em nossa compreensão de nosso próprio lugar no mundo e como agimos e reagimos em nossos contextos sociais. Isso, com certeza, deve ser uma coisa boa. A ética não deve apenas fazer parte de qualquer currículo de tecnologia da informação, mas também deve fazer parte do currículo escolar mais geral.

De qualquer maneira que pensemos sobre a ética da máquina, é certamente uma observação inevitável que conforme a IA se torna mais forte e acordamos mais totalmente para a informação que cada vez mais habitamos, a tecnologia está tomando mais decisões por nós e essas decisões têm uma probabilidade cada vez

maior de nos impactar. Portanto, precisamos explorar como imbuir a tecnologia com alguma forma de consciência ética para informar essa tomada de decisão. Fazer o contrário seria negligente. Rosalind Picard, fundadora e diretora do Grupo de Pesquisa em Computação Afetiva do MIT, coloca assim: “Quanto maior a liberdade de uma máquina, mais ela precisará de padrões morais” (PICARD, 1997).

E não é apenas uma questão de resultados. Fundamental para nossa aceitação da tecnologia de IA em nossas vidas diárias é a questão da confiança. No centro disso estão a transparência, a responsabilidade e a confiabilidade. Somente sobre essas bases pode ser construída uma boa sociedade de IA. Uma sociedade funcional requer ressonância e a ressonância requer confiança. E no cerne disso está a simpatia e o sentimento moral, como enfatizou Adam Smith.

A ética dificilmente é inequívoca e incontroversa - não apenas existem divergências sobre a estrutura ética apropriada a ser implementada, mas há tópicos específicos na teoria ética que parecem ilidir qualquer resolução definitiva independentemente da estrutura escolhida. Finalmente, dada a diversidade dos sistemas de IA hoje e no futuro previsível e a profunda dependência do comportamento ético no contexto, parece não haver esperança de construção da ética da IA em um núcleo técnico existente. Tudo isso sugere que a pesquisa em ética de IA deve ser analisada em uma lente mais ampla da dificuldade inerente à ação inteligente em geral e do contexto social complexo em que humanos e algoritmos conviverão no futuro.

GLOSSÁRIO

Algoritmo: uma série de instruções que definem como resolver um problema ou alcançar um objetivo.

Aprendizado de máquina: permite que a tecnologia digital aja e aprenda como os humanos, melhorando seu aprendizado de maneira autônoma ao longo do tempo. Isso é obtido fornecendo um fluxo de dados e informações na forma de observações e interações no mundo real.

Aprendizado profundo: uma técnica de aprendizado de máquina baseada no aprendizado, por exemplo: As tarefas são realizadas repetidamente com pequenas mudanças sendo feitas, avançando em direção a resultados cada vez mais bem-sucedidos, em uma forma de aprendizagem por tentativa e erro.

Big data: a vasta gama de dados coletados pela Internet das coisas. Sua tendência é ascendente, com aumento de volume, variedade e velocidade.

Deontologia: Uma forma de livro de regras de ética, em que uma ação é certa ou errada e as consequências da ação são irrelevantes em termos de tomada de decisão.

Existencialismo: escola de filosofia que enfatiza que o mundo não é um sistema ordenado e determinado, entendido por meio da construção de leis baseadas na observação. As atividades mundanas são consideradas fúteis e a responsabilidade pessoal é a chave. A sociedade é vista como um artefato e, muitas vezes, uma força negativa. O indivíduo deve determinar sua própria jornada, livre da sociedade, do estado ou da religião.

Humanismo: uma escola filosófica que enfatiza o valor e a agência dos seres humanos.

IA forte: significa o mesmo que inteligência geral artificial (AGI), IA forte é uma forma de IA que pode pensar como um ser humano e ser igual em toda a capacidade intelectual e desempenho. As capacidades devem incluir resolução de problemas, comunicação, planejamento, estratégia, tomada de decisão, melhoria e sensibilidade. Claro, uma vez que os humanos variam em suas capacidades intelectuais e modos de pensar, não está claro exatamente qual humano seria comparado à máquina como um padrão.

IA fraca: a IA fraca não atinge a autoconsciência ou demonstra uma ampla gama de habilidades cognitivas humanas que um ser humano pode ter. IA fraca refere-se a sistemas que são programados para realizar uma ampla gama de problemas, mas operam dentro de uma gama de funções pré-determinada ou pré-definida. Por exemplo, um AI pode ser capaz de jogar xadrez, mas ser incapaz de fazer qualquer outra coisa.

IA não simbólica: em vez de fornecer regras fixas sobre como lidar com dados, esta abordagem envolve fornecer dados ambientais brutos para a máquina e, em seguida, a máquina é deixada para reconhecer padrões, criando suas próprias representações complexas dos dados brutos fornecidos a ela. A confiança está no hardware (uma rede neural) e não no software (um programa). O aprendizado de máquina permite que a IA desenvolva suas próprias estratégias e o processo exato é inverificável e descaracterizável.

IA simbólica: entidades do mundo real são representadas com símbolos e os problemas são resolvidos usando esses símbolos de forma lógica. A IA é programado com instruções e regras exatas sobre como gerenciar esses símbolos em uma abordagem se / então. As saídas são completamente previsíveis a partir das entradas, já que os processos intermediários são determinados pelo programador humano.

Infosfera: o mundo da comunicação, onde a informação é recolhida, trocada, analisada e utilizada. Uma ênfase particular na comunicação digital, em que a era digital criou um universo paralelo, no qual somos representados como avatares de nós mesmos. A infosfera e o mundo real estão se tornando interligados.

Inteligência artificial: uma área da ciência da computação que enfatiza a criação de agentes inteligentes, pensando, funcionando e respondendo como humanos. Esses agentes são capazes de perceber seu ambiente, interpretar esse input, agindo de forma a maximizar resultados de sucesso e cumprimento de metas e aprender com a experiência.

Inteligência geral artificial (AGI): máquina capaz de resolver qualquer tarefa que um ser humano possa resolver. AGI tem a capacidade de senciência, cognição e funcionamento potencialmente muito antes do que os humanos são capazes, conhecido como superinteligência. Veja também AI forte.

Internet das coisas: bilhões de dispositivos inteligentes interconectados, todos reunindo e distribuindo grandes quantidades de dados pela Internet. Estes espertos dispositivos estão se tornando cada vez mais invisíveis e são encontrados em todo o nosso mundo, fornecendo os olhos e ouvidos da infosfera.

Leis de Asimov: as quatro leis foram desenvolvidas como parte da escrita de ficção científica de Isaac Asimov. A primeira lei afirma que um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano seja ferido. A segunda lei afirma que um robô deve obedecer às ordens dadas a ele por seres humanos, exceto quando tais ordens entrarem em conflito com a primeira lei. A terceira lei afirma que um robô deve proteger sua própria existência, desde que tal proteção não entra em conflito com a primeira ou segunda lei. A lei zero, acrescentada alguns anos depois, afirma que um robô não pode prejudicar a humanidade ou, por inação, permitir que a humanidade sofra algum dano.

Marxismo: o sistema de socialismo do qual a característica dominante é a propriedade pública dos meios de produção, distribuição e troca. A luta de classes é um elemento central, com a revolução sendo chamada para derrubar o sistema capitalista, levando a uma sociedade sem classes e autogovernada.

Trade-offs: quando existem dois ou mais desafios relacionados a um problema, é impossível otimizar a solução para todos os desafios. Os trade-offs são necessários para se obter uma solução geral. Por exemplo, uma perua não será tão aerodinâmica quanto um esportivo, mas terá mais espaço para bagagem. O compromisso é importante se uma solução for encontrada.

Utilitarismo: uma escola de ética em que os resultados determinam se algo está certo ou errado. Isso representa a posição oposta à defendida pela deontologia.

REFERÊNCIAS

Barnosky, A.D. Does evolution dance to the red queen or the court jester? Journal of Vertebrate Paleontology 19: 31ª, 1999.

Bonnefon, J.-F., Shariff, A. and Rahwan, I.. The social dilemma of autonomous vehicles. Science 352(6293): 1573-1576. 2016. Disponível em: https://arxiv.org/ftp/arxiv/ papers/1510/1510.03346.pdf Acesso: mai 2021.

Bostrom, N. and Yudkowsky, E. The ethics of artificial intelligence. The Cambridge Handbook of Artificial Intelligence. 2014.

CERNA Opinion. Éthique de la recherche enrobotique. (In French). Allistene, Paris, France. 2014. Disponível em: http://cerna-ethics-allistene.org/ digitalAssets/38/38704_Avis_robotique_livret.pdf Acesso: mai 2021.

Firth, R. (. Ethical absolutism and the ideal observer. Philosophy and Phenomenological Research, 1952.

Gould, S.J. Wonderful Life: The Burgess Shale and the Nature of History. New York: WW Norton and Company, 1990.

Grinbaum, A., Chatila, R., Devillers, L., Ganascia, J.-B., Tessier, C. and Dauchet, M.. Ethics in robotics research. CERNA mission and context. IEEE Robotics and Automation Magazine, 2017.

Gunkel, David J. Robot rights. Cambridge, MA MIT Press, 2018.

Kant, I. Groundwork of the Metaphysics of Morals (translated by Wood). A.R. New Haven, CT: Yale University Press, 2002.

LaChat, M.R.. Artificial intelligence and ethics: An exercise in the moral imagination. AI Magazine 1986.

Picard, R.. Affective computing. Cambridge, MA: MIT Press, 1997.

Prahbu, R. Big data – Big trouble? meanderings in an uncharted ethical landscape. In: Fossheim H. and Ingierd H. (eds.), Internet Research Ethics. Hellerup: Cappelen Damm Akademisk, 2015.

Smith, Adam. A riqueza das nações: uma investigação sobre a natureza e as causas da riqueza das nações / Adam Smith ; tradução Norberto de Paula Lima. -- [4. ed.]. -- Rio de Janeiro : Nova Fronteira, 2017.

Richardson, K. An Anthropology of Robots and AI: Annihilation, Anxiety and machines. Abingdon: Routledge, 2015.

Yampolskiy, R.V. Artificial intelligence safety engineering: Why machine ethics is a wrong approach. In: Müller, V.C. (ed.), Philosophy and Theory of Artificial, 2013.

HERANÇA DIGITAL: PROBLEMÁTICA NA SUCESSÃO DA BITCOIN

Walney Rodrigues Vasconcelos[1]
Ana Virgínia Cartaxo Alves[2]

1 INTRODUÇÃO

Culturalmente, o povo brasileiro não fala sobre a morte. Existe um certo tabu em falar sobre a única certeza da vida. Tampouco fala-se na divisão patrimonial pós morte. O "problema" da partilha sempre recai sobre os herdeiros, somente sendo discutida em sede de inventário, onde poderia ter sido facilitada pelo de cujus.

Em todos os campos, a ciência do direito modifica-se com uma velocidade cada vez mais rápida. Seja no Direito Penal, com as novas modalidades de crimes, sobretudo cometidos virtualmente. Seja no Direito Eleitoral através das novas ferramentas que possibilitam o exercício da cidadania. Seja no Direito Administrativo, com as novas formas da gestão pública. Seja no Direito Processual, sendo amparado pela tecnologia para dar mais rapidez e eficiência aos atos do processo. Todas essas modificações, quase sempre, se relacionam com o avanço da tecnologia.

Não obstante, o Direito Civil também tenta acompanhar o ritmo das alterações mundanas. Atualmente, questões que afetam o direito privado são as referentes à guarda de animais e seus respectivos direitos sucessórios; responsabilidade civil no meio virtual; questões envolvendo gênero. No sub-ramo do direito das sucessões também existem celeumas a exemplo da sucessão em casos de multiparentalidade.

Ainda sobre o campo do direito das sucessões, os bens que integram o espólio vêm se modificando quanto a sua forma e natureza. Ao longo da história cada vez mais bens foram se integrando ao espólio. Por que não falar atualmente em rede social como bem deixado pelo falecido? O bem, assim como outros ramos da vida, vem deixando de integrar o espaço real para integrar o ciberespaço.

Fenômeno curioso no mundo e no Brasil foi o surgimento de diversas criptomoedas no mercado financeiro. Em 2017, segundo o Startse, portal voltado

[1] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).
[2] UNIESP Centro Universitário. Coordenação do Curso de Graduação em Direito. Rodovia BR-230, km 14, S/Nº. Morada Nova. Cabedelo-PB, Brasil (CEP 58109-303).

para empreendedores, estimou- se que existem, aproximadamente, 1195 tipos de criptomoedas no mundo. Recentemente, no ano de 2018, segundo notícia divulgada pelo portal de notícias InfoMoney, até o ex-jogador Ronaldinho Gaúcho divulgou que lançará a sua, chamada de RSC (Ronaldinho Soccer Coin).

Dados divulgados recentemente pelo site Portal do BitCoin mostraram que o Brasil é o 7° país do mundo com mais corretoras de criptomoedas. Com cada vez mais gente adquirindo esse tipo de moeda, precisamos também pensar no futuro. E quando essas pessoas vierem a falecer, como será a partilha de tais bens? Como deve agir o juiz da vara de sucessões ao se debruçar com esse novo tipo de bem integrando o espólio? Como será feita a partilha? A quem deverá ser dada a ordem para entrega desses bens?

Alguns países querem proibir tal modalidade de moeda. Outros, como a Inglaterra, querem regulamentá-la, inclusive criando a própria criptomoeda do governo. No Brasil, existe um Projeto de Lei (PL n° 2.303/2015) tramitando desde julho de 2015, que inicialmente visava proibir o uso de bitcoins nos programas de milhagens aéreas, como o Smiles. Porém, através de um parecer emitido por Expedito Netto, deputado federal pelo PSD de Rondônia, o projeto de lei passou a proibir toda e qualquer operação com moedas digitais em todo o território nacional. Seguindo a mesma linha deste raciocínio a Comissão de Valores Mobiliários (CVM) proibiu o investimento em criptomoedas por gestores e administradores de fundos, pois não se sabe a natureza jurídica desse tipo de investimento. Todavia, este parece ser um caminho sem volta.

O cerne da questão é: se hoje uma pessoa morre, no Brasil, e tem em seu patrimônio criptomoedas, como será dará a sucessão destas? É o que pretendemos chegar ao final do presente trabalho.

Este artigo tem por objetivo geral desvendar a possibilidade da sucessão das criptomoedas e como isso será feito.

Tem como objetivos específicos os seguintes: o primeiro capítulo, tem por objetivo, explicar o que são bens e bens digitais, trazendo exemplos; o segundo capítulo tem o objetivo de explicar mais profundamente o que são as criptomoedas, suas aplicações práticas e como estão funcionando atualmente no mundo e no Brasil; o terceiro capítulo tem por objetivo trazer um panorama geral sobre o direito das sucessões no código civil, explicando o conceito de sucessão, herança e

herdeiro; quem pode ser herdeiro; as espécies de sucessão; e a sucessão testamentária; Por fim, o quarto e último capítulo explicará se a criptomoeda poderá ser bem integrante do espólio e como a sua sucessão poderá ser feita diante do cenário atual do ordenamento jurídico.

A justificativa do presente é que cada vez mais vivemos uma vida no mundo digital do que no mundo real. Com isso, o digital se entrelaça com o real e traz repercussões, inclusive no Direito.

Questão recentíssima no mundo e no Brasil é a do BitCoin. Cada vez mais ela está aparecendo e se tornando parte do cotidiano. Então surge o questionamento de como essa nova modalidade de transação financeira pode ser objeto de sucessão. Se nosso país é o 7° do mundo em corretoras de criptomoedas, a demanda está crescendo. Por isso é preciso o quanto antes se discutir tal fenômeno. O Direito não tem como acompanhar simultaneamente os fenômenos sociais e econômicos, mas é preciso iniciar o quanto antes o debate a respeito dessa questão.

Ainda que o problema não seja comum na sociedade, em breve o judiciário estará se debruçando sobre ele. Este trabalho tem o objetivo de ajudar e apontar um caminho para os aplicadores do direito em casos concretos a solucionar as demandas que lhe forem postas. O método de pesquisa adotado será o de consulta à bibliografia técnica – teses, dissertações, livros, legislação – e à bibliografia de divulgação do assunto – jornais, revistas e sites.

A pesquisa do presente trabalho tem o propósito explicativo. Explicar o que são os bens digitais, a presença deles em nossas vidas. Explicar ainda o que são as criptomoedas e se elas podem ser herdadas.

A abordagem será qualitativa, ou seja, buscando entender o conceito dos institutos, sua natureza jurídica, sua aplicabilidade prática e a possibilidade de sua sucessão.

O presente trabalho tem como problema a seguinte indagação: a criptomoeda pode ser bem integrante do espólio? Como será feita sua sucessão? É isso que, ao longo deste trabalho, se tentará responder.

2 BENS

Antes de ser conceituado o que é um bem digital, precisamos entender o significado de bem. Segundo o dicionário Priberam bens são haveres; propriedades.

Stolze e Pamplona (2012, p. 271) citando Beviláqua (1999, p. 213) afirmam que, sob o prisma filosófico, "bem é tudo quanto corresponde à solicitação de nossos desejos". Na doutrina muito se discute o conceito de bens e coisas.

Diz Washington de Barros Monteiro:

> O conceito de coisas corresponde ao de bens, mas nem sempre há perfeita sincronização entre as duas expressões. Às vezes, coisas são o gênero, e bens, a espécie; outras, estes são o gênero e aquelas a espécie; outras) finalmente, são os dois termos usados como sinônimos havendo então entre eles coincidência de significação. (MONTEIRO, 2000, p. 144)

Preferem definir assim os renomados juristas baianos o conceito de bens:

> Preferimos, na linha do Direito alemão, identificar a coisa sob o aspecto de sua materialidade, reservando o vocábulo aos objetos corpóreos. Os bens por sua vez, compreenderiam os objetos corpóreos ou materiais (coisas) e os ideais (bens imateriais). Dessa forma, há bens jurídicos que não são coisas: a liberdade, a honra a integridade moral, a imagem, a vida. (STOLZE e PAMPLONA, 2012, P. 273)

Uma das classificações de bens nos interessa para definir o que são bens digitais, qual seja, a de bens corpóreos ou incorpóreos.

Como o próprio nome já infere, bens corpóreos são aqueles que têm existência material. Perceptível pelos nossos sentidos, como os bens móveis (livros, joias etc.) e imóveis (terrenos etc.) em geral [...] Em contraposição aos mesmos, encontram-se os bens incorpóreos, que são aqueles abstratos, de visualização ideal (não tangível). Tendo existência apenas jurídica, por força da atuação do Direito, encontram-se, por exemplo, os direitos sobre o produto do intelecto, com valor econômico. (STOLZE e PAMPLONA, 2012, p. 299).

Adiante, depois de conceituarmos o bem digital, poderemos ter uma melhor noção onde os bens digitais se encaixam dentro dessa classificação.

2.1 BENS DIGITAIS

Se os bens em geral não encontram conceituação na Lei, os bens digitais, assunto relativamente novo no mundo, e, principalmente, no direito, também não

encontra definição legal, cabendo aos estudiosos do direito conceitua-los. Através de uma interpretação sistêmica poderíamos encaixa-los na Lei de Direitos Autorais (Lei n° 9.610/98), em seu Art. 7°, incisos I, II, VI, VII e XIII, como bem destaca Zampier. Entretanto, alerta o autor que esta lei "...não pode pretender regular todas as minúcias que a revolução tecnológica operada nas últimas décadas está a impor ao operador do Direito" (ZAMPIER, 2017, p. 61).

> Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como:
> - os textos de obras literárias, artísticas ou científicas;
> - as conferências, alocuções, sermões e outras obras da mesma natureza; VI - as obras audiovisuais, sonorizadas ou não, inclusive as cinematográficas;
> VII - as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia;
> XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual.

Partindo para um conceito doutrinário, o supracitado autor define os bens digitais como "bens incorpóreos, os quais são progressivamente inseridos na internet por um usuário, consistindo em informações de caráter pessoal que trazem alguma utilidade àquele, tenha ou não conteúdo econômico" (ZAMPIER, 2017, p. 74).

Observa-se que a migração da vida real para a vida virtual é cada vez mais célere e inevitável. Se antes pessoas revelavam fotos e construíam álbuns com suas memorias, hoje a maioria constrói álbuns virtuais com suas memorias nas redes sociais. Se antes era sempre necessário ir a um banco para realizar transações financeiras, atualmente grande parte das transações são feitas a distância.

Logo, percebemos que existe certa subdivisão entre os bens digitais, qual seja, entre aqueles de valor econômico e os de valor sentimental ou com ambos aspectos ao mesmo tempo. É o que propõe Zampier, senão vejamos:

> O ambiente virtual, assim como ocorre no mundo não virtual, comporta aspectos nitidamente econômicos, de caráter patrimonial, bem como outros ligados inteiramente aos direitos da personalidade, de natureza existencial. Dessa forma, acredita-se que seja adequada a construção de duas categorias de bem: os bens digitais patrimoniais e os bens digitais existenciais. E, por vezes, alguns bens como esta configuração poderão se apresentar com ambos os aspectos, patrimonial e existencial a um só tempo. (ZAMPIER, 2017, p. 58)

Portanto, toda vez que um bem digital puder ser valorado é chamado de bem digital patrimonial ou econômico. Os bens digitais patrimoniais/econômicos podem ser assim conceituados:

> ...quando a informação inserida em rede for capaz de gerar repercussões econômicas imediatas, há que se entender que ela será um bem tecnodigital patrimonial [...] Cada ser humano, a partir do momento em que se tornar usuário da Internet, terá a possibilidade de vir a ser titular de uma universalidade de ativos digitais. Esse patrimônio digital dotado de economicidade, formaria a noção de bem tecnodigital patrimonial. (ZAMPIER, 2017, p. 74)

Os bens digitais econômicos aparecem das mais variadas formas, sejam em milhas aéreas, bibliotecas digitais, o valor econômico de uma rede social, em moedas digitais ou até mesmo em jogos. Em notícia divulgada, pelo sítio eletrônico TecMundo um jovem de 15 anos, na Bélgica, utilizando cartões de credito dos avós, gastou cerca de 37 mil euros no jogo “Game of War: Fire Age”, comprando itens para seus personagens no jogo. Ainda no mundo dos jogos eletrônicos, o League of Legends, jogo bastante conhecido entre os jovens, utilizada mesma sistemática de venda de itens para equipar os personagens do game. Percebamos que esse tipo de transação também pode ser configurado como um bem digital patrimonial.

Complementa o autor que “... o direito de propriedade dos bens digitais deveria gozar das mesmas faculdades jurídicas existentes para a propriedade de roupagem tradicional, previstas no Art. 1.228 do Código Civil” (ZAMPIER, 2017, p. 76). Ou seja, usar, gozar, dispor e reivindicar.

Nessa esteira de pensamento é importante ressaltar que os bens digitais patrimoniais devem respeitar a função social da propriedade, a luz do direito civil-constitucional, isto é, interpretação da codificação privada a partir de princípios e normas constantes na Carta da República. A função social pode ser encontrada no Art. 5°, inciso XXIII2, da Constituição Federal, e, do Art. 1.228, § 1°3, do Código Civil. Stolze e Pamplona, citando Gisele Hiranoka, definem bem a ideia da função social atualmente, vejamos:

> Ainda que o vocábulo social sempre apresente esta tendência de nos levar a crer tratar- se de figura da concepção filosófico-socialista, deve restar esclarecido tal equívoco. Não se trata, sem sombra de dúvida, de se estar caminhando no sentido de transformar a propriedade em patrimônio coletivo da humanidade, mas tão apenas de subordinar a propriedade privada aos interesses sociais, através desta ideia-princípio, a um só tempo antiga e atual, denominada ‘doutrina da função social. (STOLZE e PAMPLONA, 2017, p. 397)

Partindo para a segunda classificação dos bens digitais temos os bens digitais existenciais, que são bens que podem ou não ser patrimoniais, mas estão ligados diretamente aos direitos da personalidade e da dignidade da pessoa humana.

Cada ser humano, a partir do momento em que se tornar usuário da Internet, terá a possibilidade de titularizar ativos digitais de natureza personalíssima. E esse movimento é altamente comum nos dias atuais, com a proliferação tantas vezes demonstrada neste estudo das redes sociais. O sujeito irá realizar o upload de fotos, vídeos, externar suas emoções, seus pensamentos, suas ideias, sua intimidade, com um número ilimitado de pessoas. Este conjunto de atributo extrapatrimoniais digitalizados ao longo do tempo, formaria a noção de bens tecnodigital extrapatrimonial. (ZAMPIER, 2018, p. 112).

Conceituam Stolze e Pamplona o direitos da personalidade como “aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais” (STOLZE e PAMPLONA, p. 67). Isto quer dizer que esses direitos tutelam atributos do indivíduo, que fogem da esfera patrimonial como bem salientou Zampier no trecho acima e arrematam os juristas baianos no seguinte excerto:

> A ideia a nortear a disciplina dos direitos da personalidade é a de uma esfera extrapatrimonial do indivíduo, em que o sujeito tem reconhecidamente tutelada pela ordem jurídica uma série indeterminada de valores não redutíveis pecuniariamente, como a vida, a integridade física, a intimidade, a honra, entre outros. (STOLZE e PAMPLONA, p. 67)

Então, poderíamos dizer que os bens digitais patrimoniais são atributos da personalidade humana, portanto protegidos pelos direitos da personalidade (Art. 5°, inciso X4, da Constituição e Art. 12 do Código Civil5), com projeção no âmbito virtual. Destaca-se o direito a imagem, privacidade e honra que são os principais direitos que se manifestam em âmbito virtual, em uma rede social, por exemplo. Inclusive, em 2018, foi sancionada e promulgada a Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709/18 - LGPD), importante instrumento na defesa da privacidade dos cidadãos, principalmente na esfera virtual.

Por fim, como já falado acima, podem existir bens que possuem caráter patrimonial e existencial ao mesmo tempo. Um exemplo desse tipo de bem digital

são os canais da plataforma YouTube em que os produtores de conteúdo com grande número de seguidores e visualizações conseguem contratos publicitários para fazer propaganda de determinado bem ou serviço em seus vídeos. A princípio esses vídeos seriam apenas manifestação do pensamento, mas acabam também tendo um caráter econômico. Outro exemplo são as redes sociais que também são plataformas de fazer publicidade através de “influenciadores e personalidades digitais”. Recentemente, em notícia veiculada pelo site de esportes ESPN Brasil, o jogador Cristiano Ronaldo se tornou a pessoa física/natural mais seguida no mundo na rede social Instagram, em decorrência dessa visibilidade, segundo o site, uma publicação publicitária em sua rede custa US$ 700 mil (mais de R$ 2 milhões de reais). Este é um claro exemplo de um bem digital existencial-patrimonial.

Pelos conceitos e definições até aqui apontados, adianta-se que o BitCoin (espécie de moeda digital que será conceituada e explicada no capítulo 4) é um bem jurídico incorpóreo. Ademais, é um bem digital patrimonial, pois possui valor econômico.

3 BLOCKCHAIN

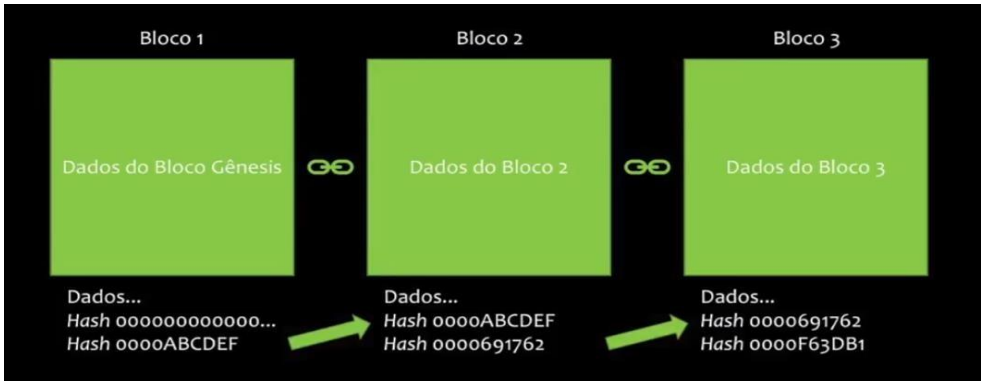
Esse capítulo tem seu conteúdo voltado mais para um lado técnico da informática, sem explanar e explorar as normas jurídicas, mas de profunda importância para entender o problema que se revela na sucessão hereditária da Bitcoin.

Não há como falar de Bitcoin sem falar de Blockchain, pois aquela precisa desta para ter funcionalidade e realizar suas transações. Para tal usaremos explicações trazidas pelo professor Matheus Passos, formado em Ciência Política e Ciência da Computação, no seu curso online denominado de “Curso Básico de Blockchain e Criptomoedas”.

Em tradução literal Blockchain significa “cadeia de blocos”. A ideia de se registrar documentos com base na data e hora nasceu em 1991 (How to time-stamp a digital document digital? – Stuart Saber e W. Scott Stornetta). Esse sistema, em palavras simples, trata-se de uma lista em crescimento continuo de registros, chamados de blocos, que são ligados uns aos outros de uma maneira segura por meio da criptografia. Começa o referido professor dizendo que o bloco é composto

por seu número (posição no bloco geral), os dados que estão ali contidos, o hash do bloco anterior e o hash do próprio bloco. O primeiro bloco é conhecido como “bloco gênesis”, fazendo a conexão de um bloco com outro através do hash do bloco anterior. O hash é uma espécie de impressão digital de cada bloco. Correspondem a um número de identificação de dados com 64 dígitos (números em formato hexadecimal – 0 a 9 e letras de A – 10 – até F – 15 – onde as letras representam números). Melhor exemplificando os dados de um bloco, temos a figura a seguir.

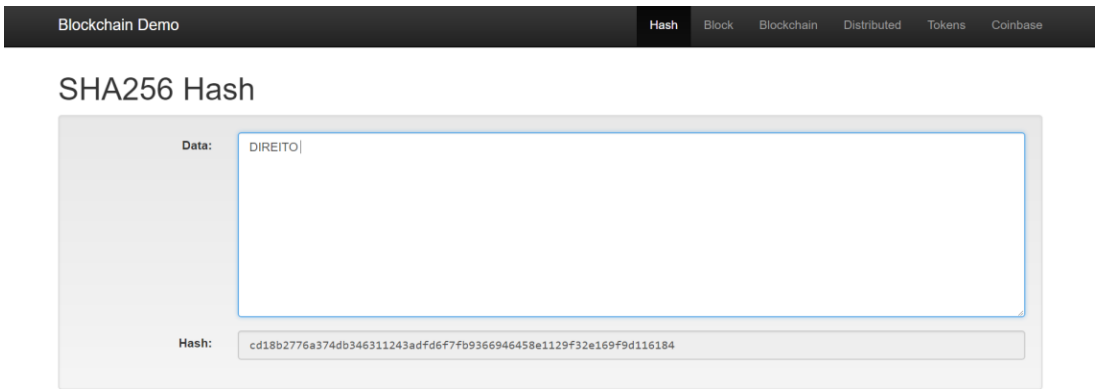
Figura 1- Funcionamento de uma Blockchain



Fonte: PASSOS (2018)

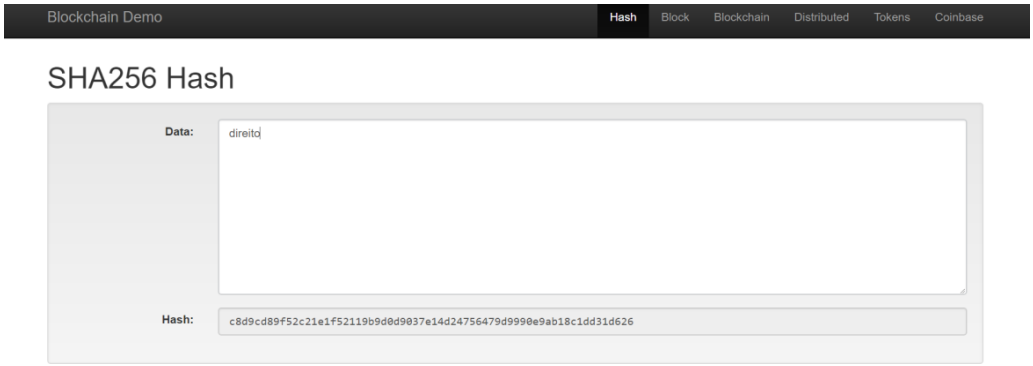
Todas as vezes que é alterado qualquer dado em um bloco o seu hash muda, ocasionando um rompimento na cadeia de blocos. Por isso o sistema de Blockchain é considerada muito seguro. Perceba-se no exemplo abaixo que a mudança no tamanho da letra altera o número do hash do bloco.

Figura 2- Exemplo de hash



Fonte: RODRIGUES (2018)

Figura 3- Exemplo de hash



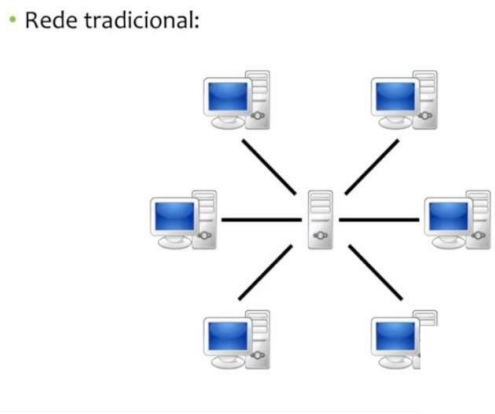
Fonte: RODRIGUES (2018)

Atualmente uma Blockchain é utilizada em diversas áreas, por exemplo, nas checagens de passaportes em aplicativos de armazenamento de senhas. Recentemente, conforme notícia divulgada pelo portal Mobile Time, um cartório na cidade de João Pessoa passou a adotar uma Blockchain para autenticação de documentos. O algoritmo funciona com qualquer tipo de documento digital, não apenas palavras ou textos, mas também para áudios, fotos, vídeos, arquivos executáveis, até um sistema operacional.

Existe a ideia de que a Blockchain é um livro razão (livro físico ou digital que contém todos os registros notariais) imutável por causa do hash. Qualquer tentativa de alteração geraria um novo hash e uma quebra na ligação dos blocos, tornando mais visíveis possíveis fraudes. Com o passar do tempo seria praticamente impossível alterar os dados gravados nos blocos. (PASSOS, 2018)

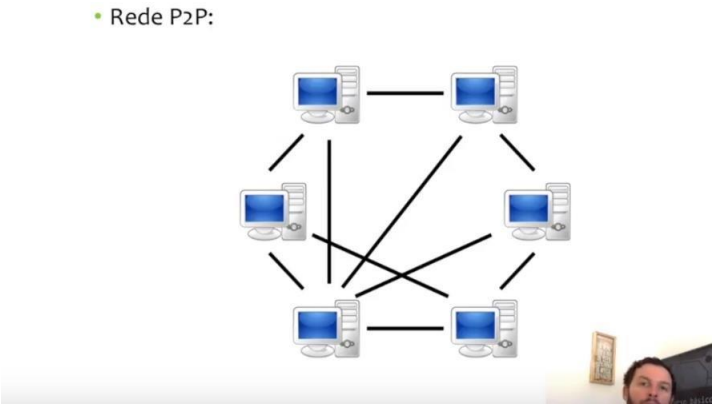
Há dois tipos de redes que podem servir de base de dados para a Blockchain: tradicional ou centralizada; e distribuída ou P2P. Essas redes servem de base dados para alimentar o sistema, parecido com um computador (servidor) utilizado para armazenar e fornecer dados para todos os outros computadores em um escritório de advocacia. No caso de uma rede centralizada (um próprio servidor) pode valer a penar alterar o conteúdo de um bloco, bem como o hash dos blocos subsequentes – dados de uma casa que valha milhões por exemplo. Ao contrário, existe a rede distribuída ou P2P em que não existe um servidor único, mas todos estão ligados ao mesmo tempo aquela rede compartilhando dados. A Blockchain está copiada em todos os computadores que estão na rede, de maneira que todos os computadores contêm uma cópia exata de todo o conteúdo da Blockchain.

Figura 4- Rede Tradicional



Fonte: PASSOS (2018)

Figura 5- Rede P2P



Fonte: PASSOS (2018)

Quando um novo bloco é adicionado, essa informação é disseminada pela rede e todos os computadores ligados à rede irão adicionar o bloco a sua própria cópia da Blockchain, fazendo uma checagem constante se todos os blocos estão atualizados. Com o tempo, mais blocos são adicionados à rede, tornando-a imutável. Se alguém conseguir alterar de maneira fraudulenta um bloco (e os subsequentes) em um único computador ligado à rede, a rede vai detectar que há alguma alteração, como explica Passos (2018).

Como a maioria dos computadores ligados à rede tem a mesma Blockchain que é diferente daquela que foi atacada, o computador que está em minoria irá copiar o conteúdo original que está nos demais computadores ligados à rede, restaurando o conteúdo original e impedindo a alteração fraudulenta do conteúdo. Um hacker teria de atacar pelo menos 50% + 1 dos computadores ligados à rede ao

mesmo tempo para ter sucesso em sua ação fraudulenta. Logo, quanto mais distribuída uma rede é, mais segura fica.

Como nos esclarece Ulrich:

> Ao contrário das redes usuais, em que há um servidor central e os computadores (clientes ou nós, nodes, em inglês) se conectam a ele, uma rede peer-to-peer (P2P) não possui um servidor centralizado. Nessa arquitetura de redes, cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor – cada um dos nós é igual aos demais (peer traduz-se como "par" ou "igual") –, o que permite o compartilhamento de dados sem a necessidade de um servidor central. Por esse motivo, uma rede peer-to-peer é considerada descentralizada, em que a força computacional é distribuída. (ULRICH, 2014, P.39)

E arremata São Severino sobre o funcionamento da Blockchain da Bitcoin:

> A rede compartilha um registro público chamado de "cadeia de blocos" ou "blockhain". Este registro contém todas as transações já processadas, permitindo que o computador do usuário verifique a validade de cada transação. A autenticidade de cada transação é protegida por assinaturas digitais correspondentes aos endereços enviados, permitindo que todos os usuários tenham controle total sobre o envio de bitcoins de seus próprios endereços Bitcoin. (SÃO SEVERINO, 2017, P. 350)

Ademais, a utilização de uma Blockchain pela Bitcoin evita outro problema de moedas digitais, qual seja, o do gasto duplo, como explica Ulrich:

> [...] Por exemplo, se Maria quisesse enviar 100 u.m. ao João por meio da internet, ela teria que depender de serviços de terceiros como PayPal ou Mastercard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria envia 100 u.m ao João, o PayPal debita a quantia de sua conta, creditando-a na de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. Imagine que não haja intermediários com registros históricos, e que o dinheiro digital seja simplesmente um arquivo de computador, da mesma forma que documentos digitais são arquivos de computador. Maria poderia enviar ao João 100
> u.m. simplesmente anexando o arquivo de dinheiro em uma mensagem. Mas assim como ocorre com um e mail, enviar um arquivo como anexo não o remove do computador originador da mensagem eletrônica. Maria reteria a cópia do arquivo após tê-lo enviado anexado à mensagem. Dessa forma, ela poderia facilmente enviar as mesmas 100 u.m. ao Marcos. Em ciência da computação, isso é conhecido como o problema do "gasto duplo", e, até o advento do Bitcoin, essa questão só poderia ser solucionada por meio de um terceiro de confiança que empregasse um registro histórico de transações. (ULRICH, 2014, p. 18)

Em suma, Blockchain é o sistema que serve de base para o uso de uma criptomoeda, sem ele não há como realizar as transações com as Bitcoins. Fazendo uma analogia, a Blockchain é como se fosse o caixa eletrônico de um banco ou o site ou o aplicativo do banco, isto é, serve de plataforma base para a realização de operações e transações financeiras.

3.1. CRIPTOMOEDAS E BITCOIN

Criptomoeda nada mais é do que uma moeda digital. É uma moeda porque tem valor comercial, sendo possível com ela fazer transação de valores. Digital porque não existe fisicamente, de modo que as transações ocorrem exclusivamente de maneira digital. São Severino diz que “bitcoin é tão virtual como os cartões de crédito e redes bancárias online que as pessoas utilizam todos os dias” (2017, P. 471).

Como bem destaca Zampier a respeito desse novo tipo de moeda:

> Inclusive, é de se registrar que empresas vêm criando suas próprias moedas virtuais, que podem ser compradas através de aquisições com desembolso de dinheiro real. O Banco Central Europeu, inclusive, definiu o caráter destas moedas virtuais como sendo o tipo de dinheiro digital não regulado, usualmente controlado pelos seus criadores, usado e aceito pelos membros de determinada comunidade virtual. [...] Até mesmo o Brasil, a Receita Federal já exige que a titularidade de moedas digitais conste da declaração anual de imposto de renda, sendo que o Banco Central afirma que tais moedas e sua possível conversão em real constituem um risco do usuário. [...] A mais proeminente destas moedas seria aquela denominada de Bitcoin, que pode ser considera a primeira criptomoeda descentralizada do mundo. (ZAMPIER, 2017, P. 64)

As criptomoedas em geral tem como características, segundo Passos (2018): a) Deve ser verdadeira; b) Só pode ser usada uma única vez; c) Ninguém pode dizer que é dono de uma moeda que está nas mãos de outrem. Segundo ele, essas características garantem a segurança desse tipo de moeda.

Importante esclarecer que criptomoeda é diferente de criptoativo. Criptomoeda é espécie de criptoativo, cuja função é de servir como meio de pagamento, facilitando as transações, tornando-as mais baratas e rápidas, logo, não existe a figura de um intermediário. Já os criptoativos são quaisquer ativos virtuais protegidos com criptografia.

As criptomoedas surgiram depois da crise econômica de 2008, nos Estados Unidos, com a incapacidade do governo e das instituições financeiras americanas de gerir o dinheiro. O BitCoin nasce em 2009, criada por Satoshi Nakamoto, constando suas principais ideias e regras em seu paper white, espécie de manual da moeda digital. Ela é uma versão puramente ponto-a- ponto (P2P) de dinheiro eletrônico que permite o envio de pagamentos online diretamente de uma pessoa para outra sem ter que passar por uma instituição financeira, representando a descentralização do poder financeiro. Para que possa ser transacionada, se vale daquilo que é chamado

de protocolo, que estabelece regras de como o valor pode ir e voltar de um participante a outra dentro da rede. (PASSOS, 2018)

Define assim Ulrich a BitCoin como “uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado” (ULRICH, 2014, p. 16).

O Bitcoin utiliza a criptografia (método de segurança por meio de funções matemáticas) para proteger os valores transacionados, por isso mostra-se segura para utilização no dia a dia, como já explicado em tópico anterior.

As principais ideias da Bitcoin, extraídas do seu paper white, são: a) Usuários interconectados; b) Não existe centralização; c) Os registros são feitos na Blockchain; d) A criptografia garante a segurança das transações.

O Bitcoin é a primeira solução totalmente segura para transferência de dinheiro entre usuários, pois cada transação é gravada na sua Blockchain, criando um histórico de movimentações, que é público, podendo ter acesso até mesmo ao conteúdo das transações, todavia a identidade das partes não é revelada. A validação das transações é confirmada pelos mineradores, que são as pessoas que emprestam o seu poder computacional (seus computadores) para a rede do BTC (sigla utilizada para BitCoin) e, em troca, são remunerados com ela.

Explica São Severino de forma sintética que:

> Novos bitcoins são gerados através de um processo competitivo e descentralizado chamado “mineração”. Esse processo consiste na recompensa dada aos usuários pelos seus serviços. Os mineiros de Bitcoin estão processando transações e fazendo a rede segura usando hardware especializado e coletando novos bitcoins em troca (SÃO SEVERINO, 2017, P. 566)

E complementa o mesmo autor a respeito da mineração:

> Mineração é o processo de usar capacidade de processamento para processar transações, garantir a segurança da rede, e manter todos os participantes do sistema sincronizados. Pode ser considerado como o datacenter (central de dados) do bitcoin, exceto que foi projetado para ser totalmente descentralizado, com mineradores em todos os países e nenhum em particular tendo controle sobre a rede. Este processo é chamado de “mineração” em uma analogia à mineração de ouro porque é um mecanismo temporário utilizado na emissão de novos bitcois. Porém diferentemente da mineração de ouro, a mineração de bitcoin prevê uma recompensa em troca dos serviços essenciais para operar uma rede segura de pagamentos. (SÃO SEVERINO, 2017, P. 735)

O BTC surge como resultado de um processo matemático complexo que envolve a resolução de problemas matemáticos e que exigem grande poder computacional, por isso faz- se necessário o auxílio de mineradores para validar as transações.

Existem algumas regras, contidas no paper white (manual de uso da bitocoin), sobre a mineração de BTC: a) Serão criados no máximo 21 milhões de BTC; b) Atualmente (em 2019) criam-se 12,5 BTC por cada bloco adicionado a Blockchain. c) A cada 4 anos a remuneração pela mineração cai pela metade.

Diz Passos (2018) que a maneira mais fácil de as obter é através das exchanges (corretoras), ou seja, uma plataforma digital na qual são negociados criptoativos. É importante destacar que estas, não são corretoras financeiras tradicionais e só pode haver comprar ou venda de criptoativos com os usuários da mesma corretora. Segundo o professor, é inseguro deixar Bitcoins nas corretoras, recomendando que após a compra elas sejam transferidas paras as carteiras (wallets), pois as corretoras são alvos constantes de ataques hackers e que não existe nenhuma garantia quanto a sua idoneidade, devendo serem deixados só pequenos valores para eventuais transações.

As carteiras (wallets) de Bitcoin podem ser de 3 tipos, a saber: software; hardware; ou paper. Essas carteiras têm duas chaves, uma privada e outra pública. A chave privada é a senha da carteira, enquanto a pública é a que todos podem ter, ou seja, o endereço para receber pagamentos. Quando a BTC é armazenada na corretora, ela tem a chave privada, por isso o perigo de deixar moedas armazenadas nelas. É importante frisar que a Bitcoin não fica na carteira, ela fica na Blockchain, o que fica na carteira é o endereço da Bitcoin na Blockchain.

Quanto aos tipos de carteira temos primeiramente a carteira software (software wallets), que são programas que podem ser acessados pelo computador ou pelo celular através de aplicativos. Esse tipo de carteira facilita o gerenciamento da moeda, pois está mais acessível e é capaz de gerar um backup (cópia de segurança) da chave privada, possibilitando a recuperação em caso de eventual perda do aparelho utilizado. Uma desvantagem desse tipo é que seu acesso é sempre online e, portanto, suscetível de ataques de hackers.

Já as carteiras do tipo hardware são dispositivos físicos parecidos com um pen drive. Ao contrário das carteiras software, elas não precisam de conexão online,

bastando a conexão com um computador. Esse fator traz a vantagem de menores chances de um ataque hacker, porém sempre precisará de um computador para acessá-las. Elas também oferecem a opção de backup. Sua desvantagem é o preço mais elevado em comparação com as outras.

Por último, o tipo paper wallet consiste em um pedaço de papel, contendo as chaves que são geradas através de um site. Por não utilizar a internet para acesso, por ser mais tradicional, evita ataques hackers. Seu problema é que não tem como fazer backup, logo, uma vez perdido o papel contendo as chaves não tem como recuperar as senhas.

A proteção da chave privada mostra-se de fundamental importância assim como a proteção da senha do banco. O uso de carteiras, em especial a software e hardware trazem mais segurança ao usuário, não possibilitando que ocorra, por exemplo, o que aconteceu com em um caso que tramitou perante o Tribunal de Justiça de São Paulo (processo n° 1090359- 77.2017.8.26.0100), segundo informações divulgadas pelo site de notícias Portal do Bitcoin, em que um usuário armazenou suas senhas nos serviços de email da empresa Google (gmail) e acabou hackeado, perdendo sua chave privada e 79 Bitcoins (equivalente a R$ 1.700.000,00). A decisão do caso foi no sentido de apenas condenar a empresa americana à indenização no valor de R$ 15.000,00 a títulos de danos morais, pois não foi capaz de fornecer os dados do hacker, todavia no tocante ao prejuízo sofrido pela perda das moedas ficou ao dissabor do usuário, tendo o juiz citado na decisão que a responsabilidade era do usuário, como vemos no trecho da decisão a seguir:

> Pela narrativa fática é fácil perceber que o autor deixou de excluir arquivos que contivessem a senha para o acesso à carteira de bitcoins, já que tais e-mails são recebidos sempre que realizada movimentação no sistema ou nas corretoras, revelando desídia com quantia tão elevada. Cediço que o requerente tem o dever de guarda de sua senha de acesso, para que eventos como no caso em tela não ocorram. Desta forma, demonstrado que os fatos se deram por exclusiva responsabilidade do requerente, que não observou o dever de guarda de sua senha de acesso, inexiste qualquer responsabilidade da requerida pela subtração dos bitcoins, impondo-se a quebra do nexo de causalidade em relação aos danos relativos à perda da criptomoeda. Vale ressaltar que é de conhecimento ordinário que o ambiente virtual é caracterizado, hodiernamente, pela possibilidade de perda de dados, ou mesmo de invasões hackers indevidas. Manter a senha de acesso à carteira de bitcoins no e-mail equivale, de maneira análoga, a guardar a senha bancária junto ao cartão correspondente, revelando a negligência com a qual o requerente armazenou informação confidencial, sendo-lhe imputada, por conseguinte, a culpa exclusiva pela perda do montante em criptomoedas. Revela-se, destarte, que a requerida não se

> responsabiliza pelos danos materiais sofridos pelo requerente. (DIÁRIO DA JUSTIÇA ELETRÔNICO, P. 660, 2019)

Logo, a proteção da chave privada é de vital importância para segurança das moedas possuídas pelo usuário e sua principal função é a movimentação das bitcoins que o usuário possui na Blockchain, além do papel fundamental na problemática que esse trabalho propõe a analisar e que será melhor explicitada no capítulo 5, tópico 5.2.

4 SUCESSÃO E HERANÇA

O Código Civil de 2002 (CC/02) é organizado seguindo a trajetória lógica de vida de um indivíduo. De início fala do nascimento e da personalidade. Logo em seguida fala sobre os bens, obrigações e suas formas de expressão. Depois vem a parte dos negócios, famílias e termina com a parte da morte. É esta que nos interessa nesse capítulo.

Sucessão e herança são conceitos que andam juntos, mas se distinguem. Sucessão (direito das sucessões) é o ato de suceder aquele que falece em todos os seus direitos e deveres. Herança pode ser conceituada, segundo Sílvio de Salvo Venosa citado por Flavio Tartuce, como “um patrimônio, ou seja, um conjunto de direitos reais e obrigacionais, ativos e passivos. O titular desse patrimônio do autor da herança, enquanto não ultimada definitivamente a partilhar, é o espólio” (TARTUCE, 2017, p. 35). Em resumo, herança é o patrimônio (bens e/ou dívidas) deixado pelo falecido.

Mister que o direito de herança é garantido pela Constituição Federal em seu Art. 5°, inciso XXX6, ou seja, é um direito fundamental.

Como se pode extrair do conceito de herança, ela é uma universalidade de bens, direitos e obrigações indivisível que permanece assim até a partilha. O art. 1.7917 do CC/02 afirma isso e seu parágrafo único preceitua que até a partilha os direitos dos co-herdeiros regular-se-ão pelas regras relativas ao condomínio. Se algum deles quiser vender sua parte, terá que alienar sua quota ideal, mas não os bens integrantes, o que só poderá ser feito depois da partilha. Essa massa de bens, também conhecida como espólio, não possui personalidade jurídica própria.

4.1 MODALIDADES DE SUCESSÃO

A sucessão pode ser legitima ou testamentária. A primeira decorre da forma da lei e a segunda da expressão de vontade do de cujus. A sucessão legitima ainda é a forma mais comum no Brasil. Porém, nem sempre foi assim “no Direito romano, a filha casada não herdava do pai e, no Direito grego, a filha não herdava em nenhuma hipótese. Essas leis decorriam não da lógica ou da razão e sim das crenças e da religião” (ROCHA, 2013, p. 25).

Atualmente, por meio da sucessão legitima, metade do patrimônio do falecido é “reservado” para os herdeiros necessários, quais sejam os que estão no rol do artigo 1.845 do estatuto privado: os descendentes; os ascendentes; e o cônjuge. A outra metade, ou no caso de não existirem herdeiros necessários, todo o patrimônio, pode ser destinada através de testamento a qualquer pessoa, exceto as constantes no Art. 1.814, satisfazendo dessa a vontade do testador e privilegiando o princípio da autonomia da vontade.

> Art. 1.814. São excluídos da sucessão os herdeiros ou legatários:
> - que houverem sido autores, co-autores ou partícipes de homicídio doloso, ou tentativa deste, contra a pessoa de cuja sucessão se tratar, seu cônjuge, companheiro, ascendente ou descendente;
> - que houverem acusado caluniosamente em juízo o autor da herança ou incorrerem em crime contra a sua honra, ou de seu cônjuge ou companheiro;
> - que, por violência ou meios fraudulentos, inibirem ou obstarem o autor da herança de dispor livremente de seus bens por ato de última vontade.

Importante ressaltar que, nos dias de hoje, não existe mais distinção entre filhos, direito este garantido até em âmbito constitucional, especificamente no Art. 227, § 6°, da Constituição Federal. Ainda sobre filhos, estes são os primeiros a serem chamados a suceder em concorrência com o cônjuge.

> Art. 227 [...]
> § 6º Os filhos, havidos ou não da relação do casamento, ou por adoção, terão os mesmos direitos e qualificações, proibidas quaisquer designações discriminatórias relativas à filiação.
>
> Art. 1.829. A sucessão legítima defere-se na ordem seguinte:
> - aos descendentes, em concorrência com o cônjuge sobrevivente, salvo se casado este com o falecido no regime da comunhão universal, ou no da separação obrigatória de bens (art. 1.640, parágrafo único); ou se, no regime da comunhão parcial, o autor da herança não houver deixado bens particulares;
> - aos ascendentes, em concorrência com o cônjuge; III - ao cônjuge sobrevivente;
> IV - aos colaterais.

Portanto, podemos concluir que a regra é a sucessão testamentária, sendo a sucessão legítima subsidiária. Todavia, como a sucessão testamentária não é muito utilizada na prática, a sucessão legítima acaba sendo a mais comum. Se, pelo menos nos casos de ativos digitais, a sucessão testamentária fosse utilizada com maior frequência, teríamos menos dúvidas nesse assunto que ainda está em um limbo jurídico.

4.2 SUCESSÃO TESTAMENTÁRIA

No tópico anterior, de forma rápida, vimos que existe a sucessão legítima, quando não há testamento e que segue os passos da lei, e a testamentária, que emana a vontade do testador. É sobre essa última que teceremos maiores comentários neste tópico, devida a sua importância na problemática da sucessão da BitCoin e que será demonstrada no próximo capítulo.

Primeiramente faz-se necessário conceituar o testamento. Tartuce assim o faz:

> Pode-se definir o testamento como um negócio jurídico unilateral, personalíssimo e revogável pelo qual o testador faz disposições de caráter patrimonial ou extrapatrimonial, para depois de sua morte. Trata-se do ato sucessório de exercício da autonomia privada por excelência. (TARTUCE, 2017, p. 212).

A partir desse conceito podemos perceber que o testamento é o principal ou um dos principais instrumentos de manifestação da vontade de um indivíduo, sendo através dele que podemos ver o princípio da autonomia privada sendo exercido.

Desse conceito podemos enxergar também outro importante aspecto, qual seja, que o testamento pode dispor sobre aspectos patrimoniais ou extrapatrimoniais. No capítulo sobre bens digitais vimos que eles também podem ser patrimoniais ou extrapatrimoniais (existenciais), mostrando desde já a conexão que se estabelece entre esses dois institutos, bens digitais e testamento. A respeito dessa conexão, Tartuce citando Jones Figueiredo Alves, diz:

> De efeito, a par da curadoria de dados dos usuários da internet, com a manutenção de perfis de pessoas falecidas, a serviço da memória digital, como já tem sido exercitada (Pierre Lévy, 2006), o instituto do testamento afetivo, notadamente no plano da curadoria de memórias da afeição, apresenta-se, agora, não apenas como uma outra inovação jurídica, pelo viés tecnológico. Mais precisamente, os testamentos afetivos poderão ser o instrumento, eloquente e romântico (um novo

> 'L'hymne à L'amour'), de pessoas, apesar de mortas, continuarem existindo pelo amor que elas possuíam e por eles também continuarem vivendo. (TARTUCE, 2017, p. 212)

Ilustrando o tema tratado acima, o serviço de correios eletrônico (email) da Google, o Gmail, lançou em 2013, conforme notícia do portal Exame no mesmo ano, uma ferramenta acessada através das configurações da conta que é possível definir qual o destino das correspondências eletrônicas post-mortem. Após certo tempo de inatividade definido pelo usuário, tentar-se-á contato com o usuário através de telefone ou por outro email cadastrado e se não houver resposta, as correspondências serão apagadas ou enviadas para pessoa escolhida pelo falecido.

Ressalta-se que esse tipo de testamento não segue os requisitos da lei, sendo uma espécie de testamento digital informal, entretanto nada impede que feito conforme a lei possa conter tais disposições.

Voltando ao testamento previsto no Código Civil podemos elencar algumas características: a) negócio jurídico; b) negócio jurídico unilateral; c) negócio jurídico gratuito;

d)negócio jurídico mortis causa; e) ato formal; f) ato revogável. É um negócio jurídico pois é uma manifestação de vontade, com conteúdo amparado pelo direito e tem uma finalidade específica. É negócio jurídico unilateral porque basta a vontade do testador para que ele se aperfeiçoe. É gratuito pois não existe vantagem para o testador, somente para o herdeiro ou legatário, dispondo de seu patrimônio, para que após sua morte, terceiro seja beneficiado sem ele receber nada em troca. Negócio jurídico mortis causa é só ter efeito após a morte do testador. É negócio formal uma vez que a lei estabelece requisitos para sua validade. Pode ser revogado ou alterado a qualquer tempo durante a vida do testador, salvo o reconhecimento de filho (Art. 1.610, CC/02)8. Por fim, ele é ato personalíssimo, isto é, cada pessoa faz seu testamento, não sendo admitido testamento conjunto no direito pátrio (Art. 1.863, CC/02)9

No tocante a capacidade de testar, ou seja, quem pode testar, a codificação civil diz que qualquer pessoa capaz tem essa prerrogativa (Art. 1.857)10. Um pouco mais adiante, no Art. 1.860, traz pessoas que não podem testar, quais sejam: incapazes; e os que "no ato de fazê-lo, não tiverem pleno discernimento". Com as alterações promovidas pelo Estatuto da Pessoa com Deficiência (Lei n° 13.146/15),

só são absolutamente capazes são os menores de 16 anos (Art. 3°, CC/02). Já os relativamente incapazes (Art. 4°, CC/02), ou seja, aqueles que precisam de assistência para realizar negócios jurídicos, são: “os maiores de dezesseis e menores de dezoito anos; os ébrios habituais e os viciados em tóxico; aqueles que, por causa transitória ou permanente, não puderem exprimir sua vontade; os pródigos”. Importante destacar que no parágrafo único do artigo 1.860 traz uma regra especial que concede capacidade testamentária aos maiores de 16 anos, portanto, excetuando a regra do Art. 4°, inciso I.

Quanto às pessoas que podem ser beneficiárias do testamento podemos dizer que são as já nascidas ou já concebidas na época da abertura da sucessão (Art. 1.798), isto é, a época do falecimento. Ainda podem ser beneficiárias do testamento, segundo o Art. 1.799: “os filhos, ainda não concebidos, de pessoas indicadas pelo testador, desde que vivas estas ao abrir-se a sucessão; as pessoas jurídicas; as pessoas jurídicas, cuja organização for determinada pelo testador sob a forma de fundação”.

E logo após vem o rol de pessoas que não podem ser beneficiárias do testamento, constante no Art. 1.801, a saber:

> Art. 1.801. Não podem ser nomeados herdeiros nem legatários:
> - a pessoa que, a rogo, escreveu o testamento, nem o seu cônjuge ou companheiro, ou os seus ascendentes e irmãos;
> - as testemunhas do testamento;
> - o concubino do testador casado, salvo se este, sem culpa sua, estiver separado de fato do cônjuge há mais de cinco anos;
> - o tabelião, civil ou militar, ou o comandante ou escrivão, perante quem se fizer, assim como o que fizer ou aprovar o testamento.

Superado esse ponto, podemos dizer que existem espécies de testamento comuns e especiais. Os comuns se subdividem em públicos, cerrados e particulares. Os especiais são: marítimo, aeronáutico e militar.

Iniciando a análise dos testamentos comuns ou ordinários temos o público, que é aquele em que o testador se dirige ao tabelionato de notas e exprime sua vontade. O tabelião ou seu substituto legal, depois de redigir o instrumento em livro próprio, deve lê-lo em voz alta para o testador e para duas testemunhas, “a um só tempo; ou pelo testador, se o quiser, na presença destas e do oficial” (BRASIL, 2002). Após a leitura todos, inclusive o tabelião, deverão assinar o testamento. Como o próprio nome já diz essa modalidade é pública, levando a ideia de que qualquer pessoa poderia ter acesso ao conteúdo do testamento dirigindo-se ao

tabelionato de notas, todavia, Tartuce pondera essa linha de pensamento trazendo regra constante em resolução do Colégio Notarial do Brasil – Conselho Federal (CNB-CF), a saber:

> Em complemento, ainda de acordo com a norma administrativa vigente, a informação sobre a existência ou não de testamento somente será fornecida pelo CNB-CF nos seguintes casos: a) mediante requisição judicial ou do Ministério Público, gratuitamente; b) de pessoa viva, a pedido do próprio testador, mediante apresentação da cópia do documento de identidade; c) de pessoa falecida, a pedido de interessado, mediante apresentação da certidão de óbito expedida pelo Registro Civil de Pessoas Naturais. Como se nota, abre-se a possibilidade de o Ministério Público ter acesso ao conteúdo do testamento, o que é um Abrandamento... (TARTUCE, 2017, p. 232)

Partindo para a segunda espécie de testamento ordinário, temos o testamento cerrado. Cerrado traz a ideia de fechado11, o que significa a principal característica dessa modalidade. Portanto, o testador vai até o tabelionato de notas e entrega seu testamento ao tabelião perante 2 testemunhas. O testador precisa declarar que aquele é seu testamento e quer sua aprovação, em seguida o tabelião vai lavrar um auto de aprovação e ler este para o testador e as testemunhas. Por fim, todos irão assinar o auto de aprovação. Como se vê, o conteúdo do testamento não é sabido por ninguém, somente pelo testador, por isso ele fechado.

Por último temos o testamento particular, que é aquele em que o testador redige e não precisa de tabelião para formalizar o ato. Justamente pela dispensa desse requisito é que, apesar de ser a forma mais simples de testar, é também a menos segura. A facilidade nessa forma não significa dizer que não existam requisitos legais. Pois bem, o testador deverá confeccionar o instrumento testamentário, ler em voz alta perante 3 testemunhas e assiná-lo, ato contínuo todas as testemunhas também deverão fazê-lo. O Código Civil traz exceção a essa regra dizendo que “em circunstâncias excepcionais declaradas na cédula, o testamento particular de próprio punho e assinado pelo testador, sem testemunhas, poderá ser confirmado, a critério do juiz” (BRASIL, 2002).

A respeito do tema foi editado o enunciado n° 611 na VII Jornada de Direito Civil, promovida pelo Conselho da Justiça Federal em 2015, com o seguinte conteúdo: “O testamento hológrafo simplificado, previsto no art. 1.879 do Código Civil, perderá eficácia se, nos 90 dias subsequentes ao fim das circunstâncias excepcionais que autorizam a sua confecção, o disponente, podendo fazê-lo, não

testar por uma das formas testamentárias ordinárias" (CFJ, 2015). Esclareça-se que a expressão "testamento holográfico" é uma expressão utilizada para testamento particular. Esse requisito da confirmação, após o prazo de 90 dias, é similar ao que veremos logo menos nos testamentos especiais.

Passando a análise da outra espécie de testamento, a especial, temos primeiramente o testamento marítimo, cujo a codificação civil foi clara em sua definição, in verbis:

> Art. 1.888. Quem estiver em viagem, a bordo de navio nacional, de guerra ou mercante, pode testar perante o comandante, em presença de duas testemunhas, por forma que corresponda ao testamento público ou ao cerrado.
> Parágrafo único. O registro do testamento será feito no diário de bordo.

Duas importantes observações faz Tartuce a respeito desse testamento: todos os comandos da lei devem ser observados, sob pena de nulidade; e que esse testamento só se justifica se a embarcação estiver em navegação (Art. 1.892), pois uma vez parada o testador deverá observar as espécies tradicionais (TARTUCE, p. 241).

Parecido é o testamento aeronáutico, com redação também clara em sua definição no artigo 1.889: "Quem estiver em viagem, a bordo de aeronave militar ou comercial, pode testar perante pessoa designada pelo comandante, observado o disposto no artigo antecedente" (BRASIL, 2002). O artigo antecedente é o que trata do testamento marítimo.

Sobre a similitude do enunciado ora citado com a codificação privada pode ser vista no artigo 1.891, senão vejamos:

> Art. 1.891. Caducará o testamento marítimo, ou aeronáutico, se o testador não morrer na viagem, nem nos noventa dias subsequentes ao seu desembarque em terra, onde possa fazer, na forma ordinária, outro testamento.

Trazendo a última forma de testamento especial temos o militar, que de igual forma foi definido pelo Código Civil.

> Art. 1.893. O testamento dos militares e demais pessoas a serviço das Forças Armadas em campanha, dentro do País ou fora dele, assim como em praça sitiada, ou que esteja de comunicações interrompidas, poderá fazer-se, não havendo tabelião ou seu substituto legal, ante duas, ou três testemunhas, se o testador não puder, ou não souber assinar, caso em que assinará por ele uma delas.

> § 1° Se o testador pertencer a corpo ou seção de corpo destacado, o testamento será escrito pelo respectivo comandante, ainda que de graduação ou posto inferior.
> § 2° Se o testador estiver em tratamento em hospital, o testamento será escrito pelo respectivo oficial de saúde, ou pelo diretor do estabelecimento.
>
> § 3° Se o testador for o oficial mais graduado, o testamento será escrito por aquele que o substituir.

Antes de partimos para o próximo capítulo, faz-se necessária uma reflexão trazida pelo autor mineiro citado neste capítulo a respeito do cenário sucessório atual.

Na verdade, tais formas especiais quase ou nenhuma aplicação prática têm, até porque encerram tipos bem específicos, de difícil concreção no mundo real contemporâneo. Se no Brasil já não são comuns os testamentos ordinários ou comuns, imagine-se a pouca incidência das formas emergenciais... (TARTUCE, 2017, p. 222)

Logo, entender essas definições básicas dessas espécies testamentárias servirá para compreender melhor as dificuldades práticas na sucessão da bitcoin e qual melhor modalidade a ser escolhida.

5 PROBLEMA FÁTICO X POSSÍVEL SOLUÇÃO

Diante do exposto até aqui, faz-se necessário alguns apontamentos a respeito do que esperar em matéria legislativa sobre o tema, qual é o real problema prático existente na atualidade e o papel do testamento diante dessa situação. É o que se verá a partir de agora.

5.1 PERSPECTIVA LEGISLATIVA

Primeiramente, desenvolvem-se alguns comentários sobre a perspectiva legislativa a respeito dos bens digitais e sua respectiva sucessão.

É certo que ainda não há nenhuma legislação vigente que trate da temática da herança digital. Nem mesmo o Marco Civil da Internet (Lei n° 12.965/14), que é

uma lei recente, foi capaz de tratar do tema, como bem nos esclarece Carvalho e Godinho no trecho a seguir:

> Neste linear, cumpre anotar, de introdutória forma, que, para além da preocupação da tutela dos conteúdos digitais ainda em vida, a inquietação deve se declinar, de igual modo, para a percepção de que a 'legislação sucessória brasileira está em descompasso com a sociedade atual', o que justifica a reformulação da matéria, assim como a necessidade do 'planejamento sucessório funcionalizar o Direito das Sucessões'. (CARVALHO e GODINHO, 2019, P. 142)

E alertam os mesmos autores que a lacuna existente no plano da herança digital não é só do legislador, "mas sobretudo dos civilistas (precipuamente os operadores do Direito Sucessório), que, em sua maioria, não se atentaram, ao menos de efetivo, para a importância do reconhecimento dos bens digitais e da sua projeção no plano sucessório" (CARVALHO e GODINHO, 2019, P. 142).

É sabido que nem só da letra da lei vive o direito, cabendo ao jurista interpretá-la e usar, por exemplo, a analogia para aplica-la as situações concretas. No caso dos bens digitais existenciais, a aplicação do capítulo referente aos direitos da personalidade do CC/02 se mostra perfeitamente possível, pois como mostrado em capítulo anterior, esse tipo de bem digital está intimamente ligado à personalidade do indivíduo. O mesmo não podemos falar dos bens digitais patrimoniais, pois em que pese em grande parte poderem serem disciplinados pelas regras já existentes, surgem outros problemas práticos advindos da tecnologia, como será explicitado um pouco mais adiante.

Se ainda não existe nenhuma previsão legal a respeito do tema, temos alguns projetos que tratam dele. Pode ser citado o Projeto de Lei n° 4.847, de 2012, que se encontra arquivado, mas que pretendia acrescentar o Capítulo II-A ao Livro V (Do Direito das Sucessões) do CC/02. Esse projeto previa o acréscimo de três artigos (1.797-A a 1.797-C) a Codificação Civil e estabelecia algumas normas básicas sobre a herança digital, como o que compõem a herança digital, sua transmissão, entre outros. Esse projeto teve mesmo conteúdo veiculado no Projeto de Lei n° 8.562, de 2017, e também teve o mesmo destino de seu antecessor, ou seja, seu arquivamento em janeiro de 2019.

De forma menos abrangente o Projeto de Lei n° 4.099, de 2012, pretende alterar o Art.

1.788 do CC/02 para passar a ter a seguinte redação:

> Art. 1.788 . .....
> Parágrafo único. Serão transmitidos aos herdeiros todos os conteúdos de contas ou arquivos digitais de titularidade do autor da herança. (BRASIL, 2012, P. 1)

Desde o ano de 2013 esse projeto aguarda para ser enviado, pela Mesa Diretora da Câmara dos Deputados, ao Senado Federal para sua análise. O Brasil é um país burocrático e moroso no que tange ao funcionamento da máquina pública, não se mostrando diferente no processo legislativo.

5.2.PROBLEMA PRÁTICO

Foi visto no capítulo 3, especificamente no tópico 3.1, que as formas de aquisição da Bitcoin podem se dá através da compra em corretoras especializadas ou através de transferências, como bem retrata São Severino ao dizer que “existem duas maneiras de comprar Bitcoins, fazendo uma transferência entre carteiras através de uma pessoa que já tem bitcoins ou através de uma corretora de moedas digitais”. (SÃO SEVERINO, 2017, P. 1003)

Interessante reflexão traz Zampier em sua obra a respeito da mudança dos bens e do eventual problema que isso pode ocasionar quando dispensado devido tratamento a eles, a saber:

> Quer seja pelo evidente valor econômico, quer seja pelo valor sentimental, os bens digitais não deveriam ser esquecidos pelos usuários da rede. Esta conduta omissiva poderá trazer uma série de problemas ligados à sucessão patrimonial ou à proteção dos direitos existências post mortem. Em breve tempo, acredita-se, tais bens serão objeto de sucessão legítima ou testamentária, cessões em vida, diretivas antecipadas, assim como ocorre com vários dos bens jurídicos que hoje são integrantes tradicionais dessas diversas formas de manifestação da vontade. (ZAMPIER, 2017, P. 66)

Também foi visto no supracitado tópico que as bitcoins de um indivíduo são armazenadas na Blockchain, mas que suas chaves privadas ficam em carteiras digitais (wallets), ficando sob responsabilidade das corretoras ou do próprio dono. Sejam elas do tipo software ou hardware é preciso ter conhecimento da chave privada para realizar transações, ficando esta chave sob o domínio do dono ou da corretora.

Quando a chave privada fica sob a responsabilidade de uma corretora de moedas digitais, parece que a questão sucessória, em caso de falecimento do dono, se mostra de mais fácil resolução. Logo, nesses casos, o juiz do caso concreto deverá determinar a corretora responsável pelos bitcoins do de cujus que partilhe em contas separadas, a fim de que seja dada a destinação da (s) moeda (s) aos seus herdeiros e legatários.

O cerne da questão e desse trabalho gira em torno da possibilidade das bitcoins serem adquiridas sem intermédio de corretoras e que o de cujus não informou sua chave privada a ninguém. Como foi visto, não é possível obter a chave de privada das carteiras sem a colaboração de quem a criou, diferentemente do que ocorre com contas de email, redes sociais, entre outras, em que é possível solicitar uma nova senha no campo “esqueci minha senha”. Para melhor compreensão da importância desse tipo de chave faz-se necessário colacionar trecho de matéria divulgada no site Portal do Bitcoin a respeito dos conceitos de chave privada, chave pública e endereço público, a saber:

> Assim, essa é a informação mais valiosa que existe para um usuário de Bitcoin e é ela que deve ser protegida para que você e mais ninguém possa ter acesso ao seu dinheiro. A chave privada é composta por até 78 números aleatórios, ou 256 bits na linguagem computacional. (SITE PORTAL DO BITCOIN, 2018)

A respeito das chaves privadas das carteiras alerta São Severino que:

> Os bitcoins perdidos ainda permanecem na Blockchain, assim como quaisquer outros bitcoins. No entanto, perder bitcoins é mantê-los perdidos para sempre, porque não há nenhuma maneira de alguém encontrar a chave privada que lhes permitiria serem gastos novamente. (SÃO SEVERINO, 2017, P. 492)

Quando a carteira utilizada pelo usuário é do tipo software, poderia ser expedido mandado judicial para a empresa que administra essa carteira solicitando a senha do de cujus e consequentemente ter-se-ia o acesso à chave privada. Já as carteiras do tipo hardware são mais seguras e, portanto, mais difíceis de serem acessadas post mortem. Para sua utilização é preciso conectá-la a um computador e para acessá-la é preciso digitar uma senha, chamada de PIN. Além desse PIN, normalmente são fornecidas 24 palavras para o usuário decorar, que funcionam como a chave privada para confirmar uma transação, pois são mais fáceis de memorizar. Esses dados são muito difíceis de acessar posteriormente porque esse tipo de carteira usa a criptografia para proteger seus dados, mostrando assim que se

o usuário não tiver deixado esses dados, dificilmente alguém conseguirá acessá-la e efetuar transações.

Por fim, a carteira do tipo paper pode ser positiva ou negativa para os sucessores. Positiva porque se ela for encontrada todos os seus dados estarão visivelmente nelas (chave pública e privada) e será possível realizar transações, entretanto, se ela não for encontrada, fica impossível saber quais são as chaves públicas e privadas se o de cujus não deixou cópia ou seus dados armazenados em outro suporte.

5.3 PAPEL DO TESTAMENTO

A sucessão testamentária, exercida através do testamento, estudada anteriormente, tem papel importante diante desse cenário de impasse e incerteza que se forma.

Antes de passarmos a questão do testamento que envolve a bitcoin, interessante ressaltar o papel do testamento existencial, tratado brevemente por Tartuce em sua obra, dizendo que “o objeto do testamento pode ser existencial, relacionado à tutela da pessoa humana, e aos direitos da personalidade, aqueles inerentes à pessoa humana, no sentido de serem originários (inatos)” (2017, P. 212). Esse tipo de testamento está intimamente ligado com os bens digitais existenciais definidos anteriormente, podendo ser utilizado pelo testador, para em vida, destinar os bens dessa natureza.

Ultrapassado esse ponto, volta-se a questão especifica que atinge o bitcoin. Como foi mostrado no tópico anterior, o cerne da questão gira em torno do conhecimento da chave privada da carteira. Nesse contexto, o de cujus poderia utilizar o testamento para destinar essa chave a um herdeiro ou legatário. Não seria recomendável que divulgasse a chave explicitamente no testamento, mas que a deixasse registrada em algum arquivo digital ou físico, sendo possível dessa maneira que seus sucessores tenham acesso as moedas digitais que compõem a herança.

De modo contrário, sem o conhecimento da chave privada fica praticamente impossível ter acesso e eventualmente partilhar o (s) bitcoin (s). Quando as moedas estão armazenadas em corretoras a questão parece se resolver mais fácil, pois uma

ordem judicial poderia ordenar que as moedas digitais do de cujus fossem repassadas aos seus herdeiros, todavia, essa forma de armazenar nem sempre mostra-se 100% segura. Primeiro porque essas corretoras podem sofrer ataques de cibercrimonosos, segundo porque a depender da forma como essas chaves são administradas internamente pela empresa, podemos nos deparar com a mesma situação de quando não é deixada a chave privada aos sucessores.

Melhor esclarecendo, conforme notícia divulgada pelo site Money Times, o CEO de uma empresa de bolsa de valores digital, no Canadá, faleceu e somente ele detinha as senhas das carteiras digitais, ficando “perdidas” moedas que somavam a quantia de aproximadamente US$ 137.000.000 (cento e trinta e sete milhões de dólares). O juiz do caso ordenou que a esposa do falecido encontrasse as senhas e não sendo possível a empresa deveria cobrir o prejuízo de outra forma. Apesar da aparente perda das moedas digitais dos clientes nesse caso, ainda é possível responsabilizar a empresa por tal fato, o que não ocorre quando o particular é quem administra diretamente suas moedas digitais e não deixa sua chave privada.

Outro fator que dificulta o uso do testamento para a solução desse problema é a questão cultural. Tartuce, citando Paulo Lôbo, fala do não costume sobre o uso do testamento dizendo que “na tradição de alguns povos, o testamento é a forma de sucessão preferencial, o que não ocorre no Brasil. Aqui, o testamento “teve sempre utilidade secundária e residual, não penetrando nos hábitos da população, como se vê na imensa predominância da sucessão legítima nos inventários abertos” (TARTUCE, 2017, p. 215).

Depois dessa análise ele fala de o porquê desse instrumento não ser tão utilizado na prática, primeiramente elencando a falta de ou pouco patrimônio da maioria dos brasileiros, do medo que as pessoas têm em falar sobre a sua morte e dos custos nos tabelionatos que registram testamentos, senão vejamos:

> Nesse contexto, conclui o presente autor que melhor seria se esse costume de não testar fosse alterado no futuro, passando o brasileiro a pensar mais no planejamento sucessório ou post mortem, especialmente porque as confusas e intrincadas regras da sucessão legítima em vigor no País não atendem mais aos anseios da sociedade, não presumindo realmente a vontade do morto. Fica o tema para as devidas reflexões dos estudiosos do Direito das Sucessões. (TARTUCE, 2017, p. 215)

Portanto, em que pese mostrar-se uma solução viável para a resolução desse problema, na prática, por todos esses fatores citados, o testamento não é

muito lembrado e utilizado. Além da evolução tecnológica que permeia a vida do indivíduo, no Brasil, seria necessário também uma evolução cultural a respeito do tema.

6 CONSIDERAÇÕES FINAIS

Ao longo desse trabalho foi visto que a evolução da tecnologia transformou diversas áreas das vidas das pessoas, a exemplo do campo econômico, incluindo as moedas. As mudanças afetam também a ciência jurídica, seja diretamente, com a digitalização dos processos, para citar um exemplo, seja indiretamente, como percebemos no tocante a questão sucessória da bitcoin.

O conceito clássico de bem foi alterado, passando atualmente a abarcar bens que aparentemente não existem, mas possuem valor existencial e econômico, que são os bens digitais. Se antigamente a ideia de bem estava ligada a um objeto tangível, como um imóvel ou um carro, hoje também pode-se dizer que uma rede social é considerada um bem digital. Se antes uma moeda física era considerada dinheiro, hoje um cartão de crédito ou uma moeda digital assume esse papel.

A ideia de Satoshi Nakamoto revolucionou o universo das moedas, criando a primeira moeda digital descentralizada. É certo que esse tipo de moeda, apesar de ainda não ser muito popular no cotidiano das pessoas, trouxe uma nova forma de realizar transações e o mais importante, de forma segura. A tecnologia Blockchain ajudou a garantir a confiabilidade da bitcoin, mas é possível ver que sua aplicação já foi expandida para diversas áreas, tornando-se uma importante ferramenta de proteção e autenticação de dados.

A utilização de moedas digitais vem crescendo gradativamente pela população. A bitcoin ajudou a popularizar essa nova forma de transação financeira, vindo depois dela diversas moedas digitais com o mesmo propósito. Logo, assim como o cartão de crédito transformou a maneira de realizar transações financeiras, as moedas digitais parecem ter assumido esse papel hoje em dia. Talvez, em futuro próximo, os cartões de crédito se tornem obsoletos face as moedas digitais, assim como o cheque se tornou obsoleto diante dos cartões de crédito.

Como grande parte das ações do homem tem reflexo no direito, não poderia ser diferente com a utilização dessas moedas. O grande cerne desse trabalho foi em

torno da possibilidade e forma de como a bitcoin poderia ser sucedida por herdeiros e legatários do de cujus.

Chega-se à conclusão de que é possível haver sucessão da bitcoin, mas não em todos os casos. Quando for adquirida através de corretoras é preciso que o juiz do processo de inventário e partilha ordene a corretora que faça a transferência das moedas existentes para as contas dos herdeiros ou legatários, ou que as transforme em dinheiro “convencional” para ser partilhado dentro do processo. Quando o de cujus pessoalmente gerenciava suas bitcoins, a solução vai depender da forma como eram armazenadas. Se em software wallet, o juiz deverá ordenar a desenvolvedora da carteira que forneça a senha de acesso a mesma, podendo posteriormente ser obtido o acesso à chave privada.

Entretanto, se o método de armazenagem for o de hardware wallet a tarefa parece mais complicada, pois esse tipo de carteira é o mais seguro, utilizando criptografia para proteção, sendo assim difícil de acessa-la por quem não conhece pelo menos o seu PIN (senha de acesso). Por fim, a paper wallet, pode ser de fácil solução, se encontrada, todavia, se não for possível encontrá-la é provável que nunca mais recupere-se as bitcoins, assim como as contidas nas hardware wallets.

A legislação atualmente existente (2019) parece não servir completamente de base legal na tratativa desse problema, devendo ser atualizada. A evolução da sociedade deve ser acompanhada pelo Direito, ainda que não concomitantemente, mas o mais rápido possível. Críticas existem, com certa razão, sobre o excesso legislativo que o Brasil possui, com diversas legislações para as mais variadas matérias, ocorre que nesse caso, sucessão hereditária de bens digitais e consequentemente de bitcoins, é preciso uma atualização das normas existentes com vistas a indicar um caminho para a resolução ou resolver efetivamente os problemas que eventualmente surjam no campo fático. Os projetos anteriormente citados são bons exemplos de atualizações legislativas que poderiam serem feitas, todavia, o desinteresse dos parlamentares por tal tema é notório, visto que tais projetos terminaram arquivados.

O testamento tem papel importante na resolução desse problema, pois se o de cujus dispor que destina suas bitcoins a determinada pessoa ou grupo de pessoas, e, deixar sua chave privada, o problema será resolvido mais facilmente. Perceba-se que é preciso que seja indicada a chave privada ou como encontrá-la,

não sendo suficiente somente a vontade. Como foi visto, a Blockchain é um sistema muito seguro e descentralizado, não sendo possível ordenar a um ente específico que transfira as bitcoins para determinada pessoa. O conhecimento da chave privada é de fundamental importância nesse processo.

Encerra-se o presente trabalho com uma reflexão sobre a questão sucessória no Brasil. A sucessão do indivíduo é pouco discutida por ele mesmo, certamente a questão cultural tendo grande influência nesse problema. Não só o homem médio não pensa e planeja sua sucessão, enfrentando tal dificuldade até mesmo os operadores do direito. O testamento mostra-se instrumento importante na sucessão, sobretudo na sucessão de bitcoin, no entanto, sua pouquíssima utilização no país torna praticamente ineficaz sua utilização como meio de solução no problema tratado ao longo desse trabalho.

É preciso mudar o pensamento da população no tocante a um fato que vai acometer a todos sem distinção, a morte. O planejamento sucessório é uma importante decisão que todos tem tomar, facilitando a vida daqueles que continuarão a existir para além da sua morte, ajudando e esclarecendo o trabalho do judiciário, tornando os processos mais céleres.

REFERÊNCIAS

BARROS MONTEIRO, Washington de. Curso de Direito Civil: Volume 1. 37ª edição. São Paulo: Saraiva, 2000.

Bitcoin: Um sistema ponto-a-ponto de dinheiro eletrônico. Embaixada Bitcoin. Disponível em: <http://www.embaixadabitcoin.com/wp-content/uploads/2017/11/Bitcoin-White-Paper- Portugues.pdf>. Acesso em: 18 out. 2018.

Blockchain é adotada para autenticação de documentos em cartório de João Pessoa.
Mobile Time. Disponível em: <https://www.mobiletime.com.br/noticias/11/10/2018/blockchain-e-adotada-para-autenticacao-de-documentos-em-cartorio-de-joao-pessoa/>. Acesso em: 01 de março de 2019.

BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm>. Acesso em: 25 de janeiro de 2019.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Disponível em:

<http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406compilada.htm>. Acesso em: 30 janeiro de 2019.

Bitcoin: Juiz dá 30 dias para esposa procurar senha perdida com morte de CEO. Money Times. Disponível em: <https://moneytimes.com.br/bitcoin-juiz-da-30-dias-para-esposa- procurar-senha-perdida-com-morte-de-ceo/>. Acessado em: 29 de abril de 2019.
Cerrado. Dicionário Priberam. Disponível em: <https://dicionario.priberam.org/cerrado>. Acesso em: 25 de março de 2019.

Chave pública e privada do Bitcoin: entenda o que são e como funcionam. Portal do Bitcoin. Disponível em: <https://portaldobitcoin.com/chave-publica-e-privada-do-bitcoin- entenda-o-que-sao-e-como-funcionam/>. Acessado em: 25 de abril de 2019.

Cristiano Ronaldo quebra mais um recorde. ESPN. Disponível em: <https://twitter.com/espnagora/status/1080907395025448960>. Acesso em: 17 de março de 2019.

Brasil, Conselho da Justiça Federal. Enunciado número 611, VII Jornada de Direito Civil. Disponível <http://www.cjf.jus.br/enunciados/enunciado/611>. Acessado em: 22 de março de 2019.

Existem 1195 versões de criptomoedas no mundo: conheça as principais. StarteSe. Disponível em: <https://www.startse.com/noticia/para-startups/40973/existem-1195-versoes- de-criptomoedas-no-mundo-conheca-as-principais >. Acesso em: 01 de março de 2018.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo curso de direito civil, volume 1: parte geral. 14. ed. rev., atual e ampl. São Paulo: Saraiva, 2012.

Garoto de 15 anos gasta mais de 100 mil reais em jogo online “gratuito”. Site TecMundo. Disponível em: <https://www.tecmundo.com.br/video-game-e-jogos/63992-garoto-15-anos- gasta-100-mil-reais-jogo-online-gratuito.htm>. Acesso em: 25 de março de 2019.

Google integra função de “testamento” a seus serviços online. Exame. Disponível em: <https://exame.abril.com.br/tecnologia/google-integra-funcao-de-testamento-a-seus-servicos- online/>. Acessado em: 18 de março de 2019.

Google vai pagar R$ 15 mil a brasileiro que perdeu R$ 1 milhão em Bitcoin após ser hackeado. Alexandre Antunes. Disponível em: <https://portaldobitcoin.com/google-pagar- 15-mil-brasileiro-perdeu-1-milhao-bitcoin-hackeado/>. Acessado em: 30 de abril de 2019.

LACERDA, Bruno Torquato Zampier. Bens digitais. Indaiatuba: Editora Foco Jurídico, 2017.

LIMA, Isabela Rocha. Herança Digital: direitos sucessórios de bens armazenados digitalmente. Disponível em:

<http://bdm.unb.br/bitstream/10483/6799/1/2013_IsabelaRochaLima.pdf>. Acesso em: 12 de agosto de 2018.

PASSOS, Matheus. Aula 1: Conceito Geral de Blockchain. 2018. (10m44s). Disponível em: https://www.youtube.com/watch?v=MnCh6KTYqZM&list=PLjz295APz97kb1ZWYFS m1Te 99zF8pZQS&index=2. Acesso em: 18 set. 2018.

PASSOS, Matheus. Aula 4: A rede distribuída P2P. 2018. (13m22s). Disponível em: https://www.youtube.com/watch?v=EIBqLJ7e0YQ&index=5&list=PLjz295APz97kb1Z WYF Sm1Te99zF8pZQS. Acesso em: 25 set. 2018.

PASSOS, Matheus. Aula 8: O que é uma criptomoeda. 2018. (22m55s). Disponível em: https://www.youtube.com/watch?v=z2IRe2ezhK0&index=10&list=PLjz295APz97kb1Z WYF Sm1Te99zF8pZQS. Acesso em: 09 out. 2018.

PASSOS, Matheus. Aula 11: Como adquirir BTC nas exchanges. 2018. (16m49s). Disponível em: https://www.youtube.com/watch?v=iYyDxeLpBDo&index=13&list=PLjz-295APz97kb1ZWYFSm1Te99zF8pZQS. Acesso em: 23 out. 2018.

Ronaldinho Gaúcho vai lançar sua própria criptomoeda. Disponível em: < https://www.infomoney.com.br/mercados/bitcoin/noticia/7517530/ronaldinho-gaucho-vai- lancar-sua-propria-criptomoeda >. Acesso em: 01 de março de 2019.

TARTUCE, Flávio. Direito civil, v. 6: direito das sucessões.10. ed. rev., atual. e ampl. Rio de Janeiro: Editora Forense, 2017.

ULRICH, Fernando. BitCoin: a moeda na era digital. São Paulo: Instituto Ludwdig von Mises Brasil, 2014.

TEIXEIRA, Daniele Chaves. Planejamento Sucessório. Belo Horizonte: Editora Fórum, 2019.

ISBN 978-655825092-0