Direito Digital
CAST

DEBATES SOBRE DIREITO DIGITAL

Coordenação Científica
Lucas Cortizo • Raphael Souza • Victor Mulin

DEBATES SOBRE O DIREITO DIGITAL

Coordenação Científica:
Lucas Cortizo, Raphael Souza e Victor Mulin

Autores:
Abrantes Malaquias Belo Caiúve | Fernanda Galera Soler |
Lucas Cortizo | Lucas Prado | Sircéia Macedo | Victor Mulin

Edição:
Direito Digital Cast

Coordenação Técnica:
Lucas Cortizo, Raphael Souza e Victor Mulin

Editor de arte:
Daniel Moreira Vidal

ISBN: 978-65-00-14718-6 | DOI: 10.29327/527673

Lisboa, Portugal

Esse é um trabalho sem fins lucrativos realizado pelo Direito Digital Cast através de um Call for Papers em que os autores enviaram seus artigos para análise e publicação.

O Direito Digital Cast apenas reuniu os melhores artigos submetidos para essa publicação, não sendo responsável pelo conteúdo dos artigos de cada um dos respectivos autores.

Os coordenadores científicos agradecem a participação e a dedicação de todos os autores na criação desta obra.

Esse livro contempla autores que estão localizados em diversos países de língua portuguesa, como Brasil, Portugal e Angola. Isso posto, e em respeito a cada um dos autores, foi mantida a língua de origem utilizada por cada autor.

Sumário

INTELIGÊNCIA ARTIFICIAL

Regulação de IA: uma apresentação sobre as propostas europeias acerca da definição jurídica e do âmbito de aplicação de um futuro quadro regulatório baseado no risco

Victor Moreira Mulin Leal[1]

Resumo:
O uso de sistemas de IA tem provocado, ao mesmo tempo, grandes oportunidades econômicas e impactos nos direitos fundamentais dos indivíduos. Esse cenário, se torna ainda mais complexo pela inexistência de uma legislação própria, adequada e específica para lidar com situações que envolvem a IA. Isso posto, é apresentado nesse artigo, a proposta europeia de regulação de IA concernente à definição jurídica de IA e a definição do âmbito de aplicação de um futuro quadro regulamentar sobre IA. Dessa forma, através desse artigo, visa-se trazer mais conhecimento para o cenário brasileiro de regulação a ponto de que possa servir de inspiração para o desafio enfrentado pelo legislador brasileiro.

Palavras-chave: Inteligência artificial; projeto de lei; inovação; legislação; desafio.

[1] Advogado e consultor nas áreas de inteligência artificial e proteção de dados no escritório Marquesini Chiavone Advocacia; mestrando em Direito e Informática pela Universidade do Minho, Portugal; mobilidade internacional no IT Law Master da Universidade de Tartu, Estônia; fundador do podcast jurídico Direito Digital Cast; investigador no grupo de pesquisa E-Tec no Centro de Justiça e Governança (JusGov) da Escola de Direito da Universidade do Minho e investigador da LAPIN em assuntos relacionados à inteligência artificial e novas tecnologias.

Introdução

Seja no Brasil ou na Europa, a digitalização das relações sociais e o grande volume de dados criados diariamente já é uma característica da sociedade atual. Os dados, principalmente aqueles de natureza pessoal, ganham cada vez mais relevo e importância, pois passaram a exercer a função de combustível no desenvolvimento e no aprimoramento de sistemas de inteligência artificial (IA). Nesse sentido, é possível afirmar que essa relação entre dados e IA tem gerado inúmeras e diversificadas oportunidades. No entanto, toda essa evolução tem cobrado um preço desproporcional dos indivíduos e da sociedade.

Afirma-se isso, pois o mau uso de sistemas de IA tem causado danos de difícil ou impossível reparação. Nesse contexto, embora a IA possa ser utilizada para aumentar nossa comodidade e melhorar nossa segurança, seus sistemas também podem ser implantados como um meio de vigilância ilegítima, onde cada vez mais se percebe problemas relacionados com a cultura da economia de vigilância que limita a privacidade dos indivíduos[2][3]. Além disso, os dados pessoais, que incialmente seriam usados para personalizar a prestação de um serviço,

[2] CLARKE, R. Profiling: a hidden challenge to the regulation of data surveillance. Journal of Law and Information Science, Australia, v. 4, n. 2, December. 1993. Available at: <http://www.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.htmlD>.

[3] Magrani, Eduardo. Entre dados e robôs "Ética e privacidade na era da hiperconectividade". Publisher Arquipélago. 2019. ISBN 978-85-5450-029-0

passaram a ser tratados indiscriminadamente para a construção de perfis psicológicos, o que coloca os titulares de dados vulneráveis a qualquer tipo de condicionamento ou manipulação[4][5]. Por fim, ainda existem riscos de que dados enviesados possam causar injustificada discriminação[6], sem, contudo, possibilitar aos usuários uma explicação dos motivos que fundamentam a decisão ou o processo decisório[7].

Como se pode perceber, os impactos negativos advindos dos sistemas de IA já geram uma profunda insegurança aos direitos e garantias protegidos por nosso ordenamento jurídico. Contudo, o cenário brasileiro se torna ainda mais complexo pela inexistência de um diploma jurídico que regule especificamente a IA. Aliás, sobre esse contexto, é importante destacar que, em que pese a existência de projetos de lei que abordem o tema IA[8], eles apenas pretendem, superficialmente, criar regras e princípios gerais e abstratos para a regulação de IA no Brasil, sem, contudo, propor uma solução factível aos desafios apresentados por essa tecnologia.

---

[4] European Data Protection Supervisor (EDPS), Opinion 3/2018 on online manipulation and personal data, March 19, 2018.
[5] Ebers, Martin, Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges (April 17, 2019). Martin Ebers/Susana Navas Navarro (eds.), Algorithms and Law, Cambridge, Cambridge University Press, 2019 (Forthcoming), Available at SSRN: https://ssrn.com/abstract=3392379 or http://dx.doi.org/10.2139/ssrn.3392379
[6] European Parliament. Artificial intelligence: From ethics to policy. EPRS | European Parliamentary Research Service. Scientific Foresight Unit (STOA). PE 641.507 – June 2020
[7] PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015
[8] Pelo que posso citar tanto o PL 21/2020 e PL 240, DE 2020, ambos da Câmara dos Deputados, quanto o PL 5051, de 2019 do Senado federal.

Isso posto, ao levar em consideração que a União Europeia (UE) é um dos agentes internacionais com maior influência sobre esse tema, o objetivo desse artigo é o de apresentar a discussão europeia sobre uma regulação baseada em risco para sistemas de IA, pelo que, possivelmente, poderá servir de inspiração para o cenário brasileiro.

1. Regulação de IA: o caminho legislativo a ser seguido

Antes de depositar todas as energias no desenvolvimento de um quadro regulamentar para a IA, é preciso que os legisladores competentes tenham conhecimento profundo do contexto e das características principais que orientam a IA.

No que se refere a parte do contexto, por mais que ainda não exista nenhuma regulamentação vinculante voltada explicitamente para IA, é importante destacar que os desenvolvedores e os responsáveis pela implantação e oferecimento de sistemas de IA já estão sujeitos à legislação relacionada a matéria de direitos fundamentais[9], sendo essa uma afirmação que se aplica tanto na Europa quanto no Brasil. Além disso, a depender do propósito e da adequação, sistemas de IA devem, desde a sua concepção, respeitar as regras de privacidade, proteção de dados, não discriminação, proteção dos

[9] Grupo de Peritos de Alto Nível em IA. Livro Branco sobre Inteligência Artificial: uma abordagem europeia de excelência e confiança.

consumidores e, principalmente, as regras relativas à segurança e responsabilidade civil. Isso posto, não se pode permitir qualquer arguição de vácuo legislativo. O quadro atual pode até não ser adequado, mas os princípios e regras devem ser devidamente aplicados.

Com isso em mente, o legislador competente deverá determinar, exatamente, o âmbito de aplicação de uma futura regulamentação jurídica acerca da IA. Para que isso seja realizado, o legislador deve começar pela proposição de uma definição acerca do que será entendido como IA. Afirma-se isso porque sistemas de IA estão em todos os setores da sociedade, possuindo utilizações de diversos níveis de importância e de impacto para a sociedade. Como um dos possíveis exemplos, ao mesmo tempo que temos sistemas de IA responsáveis para filtrar SPAM da caixa de e-mail, também temos sistemas de IA verificando prognósticos de saúde, operando com investimentos em bolsa de valores e guiando armas autônomas inteligentes.

Ultrapassado esse momento conceitual, o legislador competente poderá então definir a amplitude da aplicação de uma regulação de IA, ou seja, definir se o quadro regulamentar será, ou não, aplicado para todo e qualquer produto ou serviço que seja baseado em IA. Essa é uma discussão relevante, já que um eventual quadro regulamentar para a IA "deve ser eficaz para atingir os seus objetivos, mas não excessivamente prescritivo, de forma a não criar um encargo desproporcionado, especialmente

para as pequenas e médias empresas"[10]. Dessa forma, o legislador deverá estar atento para buscar o devido equilíbrio em proteger os direitos fundamentais das pessoas, mas, ao mesmo tempo, não promover uma restrição demasiada a ponto de impedir o desenvolvimento econômico inerente à inovação de sistemas baseados em IA.

Com esse contexto em mente, torna-se possível apresentar a proposta de regulação que tem sido discutida na União Europeia, que mais do que simplesmente regular a IA como um todo, busca apenas regular sistemas de IA que possam apresentar um risco para a sociedade e para os indivíduos.

2. Um ponto de partida para as discussões sobre uma definição europeia para a IA

Por não haver um ato normativo explícito para a IA na União Europeia, há uma discussão acerca da necessidade de somente adaptar a legislação em vigor ou desenvolver uma legislação específica sobre o tema. Independentemente da decisão a ser tomada, a primeira responsabilidade da Comissão Europeia (CE) deverá ser a construção de uma definição sobre o que será reconhecido como inteligência artificial. Destaca-se aqui uma preocupação no sentido de que essa definição deverá ser suficientemente flexível, a ponto de se adaptar a

[10] Grupo de Peritos de Alto Nível em IA. Livro Branco sobre Inteligência Artificial...

diversificação de aplicações possíveis e a eventuais progressos técnicos que a IA poderá vir a sofrer. Essa flexibilidade da definição é tida como uma característica crucial, já que proporcionará a segurança jurídica necessária para a proteção de dos direitos dos usuários e do desenvolvimento das empresas.

No que se refere a essa definição, ainda não há algo completamente sacramentado na jurisdição europeia. No entanto, o Grupo de Peritos de Alto Nível para Inteligência Artificial (GPAN IA) apresentou uma definição completa e extensa sobre o que poderia a ser entendido como sistema de IA. Essa definição pode ser encontrada em 'Uma Definição de IA: principais capacidades e disciplinas cientificas'[11]. Assim sendo, e de acordo com o GPAN IA, podemos entender os sistemas de inteligência IA como:

> "sistemas de software (e eventualmente também de hardware) concebidos por seres humanos[12], que, tendo recebido um objetivo complexo, atuam na dimensão física ou digital [percebendo] o seu ambiente mediante a aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as

[11] Grupo de Peritos de Alto Nível em IA. Uma definição de ia: principais capacidades e disciplinas científicas

[12] Os seres humanos concebem os sistemas de IA diretamente, mas também podem utilizar técnicas de IA para otimizar a sua conceção (Nota realizada pelo próprio GPAN IA).

> informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido. Os sistemas de IA podem utilizar regras simbólicas ou aprender um modelo numérico, bem como adaptar o seu comportamento mediante uma análise do modo como o ambiente foi afetado pelas suas ações anteriores"[13].

Além dessa indicação específica e direta sobre atos e ações, o GPAN IA fez questão de nominar as técnicas e as abordagens que possivelmente podem estar atreladas à IA. Nesse sentido, o GPAN IA menciona que a IA, enquanto disciplina científica, pode apresentar abordagens como:

> "a aprendizagem automática (de que a aprendizagem profunda e a aprendizagem por reforço são exemplos específicos), o raciocínio automático (que inclui o planeamento, a programação, a representação do conhecimento e o raciocínio, a pesquisa e a otimização) e a robótica (que inclui o controlo, a percepção, os sensores e atuadores, bem como a integração de todas as outras técnicas em sistemas ciberfísicos)"[14].

[13] Grupo de Peritos de Alto Nível em IA. Uma definição de IA...
[14] *Ibid*

Como se pode perceber, a definição de IA apresentada pelo GPAN IA tenta abordar, de forma ampla, os atos que permeiam quase toda e qualquer ação que um sistema de IA pode realizar. De fato, levando em consideração as possíveis evoluções da IA, é possível entender que a definição do GPAN IA alcançou a necessária flexibilidade requerida pela CE, uma vez que essa definição pode se manter eficaz ao longo do tempo e da evolução tecnologia. Além disso, essa definição também alcança uma precisão necessária, uma vez que possibilita identificar e enquadrar simples, complexas ou distintas aplicações baseadas em IA. Isso posto, pode-se afirmar que tal definição auxilia no desejo de segurança jurídica.

3. Uma perspectiva europeia para regulação de IA através de uma abordagem baseada em riscos

Ultrapassado esse momento, a segunda responsabilidade da CE será a de determinar, exatamente, o âmbito de aplicação de uma possível e futura regulamentação jurídica acerca da IA. Ou seja, deve-se definir se um futuro quadro regulamentar será, ou não, aplicado para todo e qualquer produto ou serviço que seja baseado em inteligência artificial. Dessa forma, a CE deve estar atenta para buscar o devido equilíbrio em proteger os direitos fundamentais das pessoas, mas, ao mesmo tempo, não promover uma restrição

demasiada a ponto de impedir o desenvolvimento econômico inerente à inovação de sistemas baseados em IA.

Assim sendo, com esse equilíbrio em mente, a CE propõe, através do seu Livro Branco sobre Inteligência Artificial, que o caminho regulamentar a ser seguido seja através de uma abordagem baseada em risco, onde uma regulação mais rigorosa incidirá apenas nos sistemas de IA qualificados como de «alto risco»[15]. Para que essa abordagem seja, portanto, eficaz, será necessário perceber as condições que levam uma classificação ser considerada de «baixo risco» ou de «alto risco».

No entanto, é importante destacar que a classificação somente é relevante para saber sobre a aplicação do quadro regulamentar específico sobre a IA. Isso porque, independentemente de como um sistema de IA for qualificado, tanto os de baixo quanto os de alto risco continuarão inteiramente sujeitos as regras já existentes na União Europeia, como por exemplo a necessária conformidade com o Regulamento Geral de Proteção de Dados.

De acordo com o quadro baseado em risco proposto pela CE, para um sistema de IA ser considerado de «alto risco», em regra, deverão ser analisadas duas de suas características, sendo elas o «setor» no qual o sistema é utilizado e seu respectivo «uso pretendido». Destaca-se apenas que, enquanto a análise do «setor» ocorre de forma mais objetiva, a análise do «uso

[15] Grupo de Peritos de Alto Nível em IA. Livro Branco sobre Inteligência Artificial...

pretendido» é mais subjetiva, e depende de um risco significativo que será analisado pela perspectiva da segurança, dos direitos dos consumidores ou dos direitos fundamentais[16].

Dessa forma, quando a CE se refere ao requisito «setor», isso significa dizer que a aplicação de IA é utilizada em uma área que, dadas as características inerentes a ela, é expectável se esperar pela ocorrência de riscos significativos. Como exemplo pode-se citar as áreas e os setores relacionados com os cuidados de saúde, os transportes, a energia e determinadas partes do setor público, dentre essas, asilo, migração e controlos nas fronteiras, como também o sistema judicial, a segurança social e os serviços de emprego[17].

Importante destacar que, nesse sentido, a própria CE alerta que os setores considerados de «alto risco» devem ser enumerados de forma específica e exaustiva em um futuro quadro regulamentar, e que essa lista deve ser periodicamente revista e atualizada quando necessário. Como mencionado, a análise do «setor» se dá de forma simples e objetiva, isso porque depende necessariamente de prévia indicação pelas autoridades reguladoras.

No entanto, ao que se refere ao requisito de «uso pretendido», a aplicação de IA, além de estar inserida no «setor» considerado de risco, deverá ser utilizada de tal forma que seja

[16] Grupo de Peritos de Alto Nível em IA. Livro Branco sobre Inteligência Artificial...
[17] *Ibid.*

provável que surjam riscos significativos aos seus utilizadores. De acordo com a CE, "este segundo critério reflete o reconhecimento de que nem todas as utilizações da IA nos setores selecionados implicam necessariamente riscos significativos"[18]. Como mencionado, essa é uma análise subjetiva, uma vez que o risco do sistema será avaliado através de várias perspectivas legais e de segurança.

Contudo, há uma observação importante a ser feita. Isso porque a classificação como de «alto risco» depende da ocorrência de um requisito duplo. Ou seja, para ser classificado como um sistema de IA de «alto risco», este deverá ter tanto o seu «setor» de utilização quanto o seu respectivo «uso pretendido», em conjunto, caracterizados como de risco elevado.

Para poder melhor ilustrar a abordagem baseada em risco, um exemplo dado pela própria CE refere-se a seguinte situação: um sistema de IA na área da saúde (setor) implica, em um primeiro momento, um dos mais altos níveis de riscos aos direitos fundamentais, e por isso, em tese, qualquer aplicação de IA seria reconhecida como de «alto risco». No entanto, se nesse contexto a aplicação de IA for apenas responsável pela organização da triagem de atendimento (uso pretendido), sem que implique direto e elevado risco aos usuários, não poderá, portanto, ser o sistema inteligente reconhecido como de «alto risco».

[18] Grupo de Peritos de Alto Nível em IA. Livro Branco sobre Inteligência Artificial...

No entanto, com a intenção de evitar um possível excesso de rigidez do âmbito de aplicação, a própria CE já previu a possibilidade de existirem alguns casos excepcionais que representam alto risco e que possam ocorrer fora de setores previamente reconhecidos. Nesse sentido, de acordo com a CE, o próprio «uso pretendido» já representa um risco evidentemente alto, o que torna irrelevante o «setor» de aplicação em causa. Como exemplo, a CE menciona aplicações de IA que afetem os diretos dos trabalhadores, que sejam relacionadas as matérias de igualdade de emprego ou processos de recrutamento. Além disso, também são citadas aplicações cuja utilização gere efeitos de identificação biométrica à distância[19] ou de tecnologias de vigilância intrusivas, onde todos esses exemplos seriam sempre considerados de alto risco.

Dessa forma, é importante destacar que a abordagem baseada em risco, com a necessidade de presença de dois critérios cumulativos (ou identificação de uma das possíveis exceções), garante que o âmbito de aplicação do quadro regulamentar seja bem delimitado, proporcionando assim segurança jurídica para as empresas. Além disso, o estrito âmbito de aplicação incentiva o uso e desenvolvimento de IA

[19] A identificação biométrica à distância deve ser distinguida da autenticação biométrica (esta última é um processo de segurança que depende das características biológicas únicas de uma pessoa para verificar se é quem afirma ser). A identificação biométrica à distância ocorre quando as identidades de várias pessoas são estabelecidas com a ajuda de identificadores biométricos (impressões digitais, imagem facial, íris, padrões vasculares, etc.) à distância, num espaço público e de forma contínua ou permanente, mediante a sua verificação em comparação com dados armazenados numa base de dados

pelas pequenas e médias empresas, uma vez que, cientes do baixo risco de aplicações que queiram utilizar, não sofreram com mais encargos legislativos mais rigorosos. Por outro lado, a delimitação baseada em risco também permite que as autoridades e os agentes responsáveis efetuem um trabalho fiscalizatório mais específico e profundo em sistemas de alto risco, o que contribui para a proteção dos diretos fundamentais dos usuários.

Considerações finais

O uso de sistemas de IA por todos os setores da sociedade tem provocado grandes oportunidades econômicas, mas também tem ocasionado impactos nos direitos fundamentais dos indivíduos. Esse cenário, que provoca diversos reflexos jurídicos, se torna mais complexo pela inexistência de uma legislação própria, adequada e específica para lidar com situações que envolvem a IA. Isso posto, tanto no Brasil quando na União Europeia, o grande desafio enfrentado pelos legisladores é o de propor uma regulação específica para a IA.

Como foi mencionado, o Brasil atualmente apresenta algumas propostas de lei com essa finalidade. Contudo, tais propostas ainda figuram em um estado amplo e abstrato, guiado principalmente por princípios norteadores para a IA. Assim sendo, tendo em consideração a necessidade de entender o

contexto inerente à regulação da IA, o trabalho se propôs a apresentar os desenvolvimentos que tem sido realizado na União Europeia, restringindo o foco do estudo em dois aspectos super importantes, sendo eles a própria definição jurídica de IA e a definição da amplitude do âmbito de aplicação de uma regulação específica sobre esse tema.

No que se refere à definição jurídica de IA, foi levantada a necessidade de criação de uma definição que possa promover segurança jurídica para todos os envolvidos, seja desenvolvedores, utilizadores e sociedade. Essa segurança jurídica, como mencionado, advém da necessária flexibilidade do conceito de IA, isso porque, como exemplificado, sistemas inteligentes podem ser encontrados desde sistemas de filtro de SPAM até armas autônomas inteligentes. Além disso, a mesma definição deve ser eficaz ao longo do tempo, tendo em vista a evolução da tecnologia.

Isso posto, a fim de ir ao encontro dos requisitos ambicionados, foi apresentada uma definição de IA proposta no cenário europeu pelo GPAN IA. E, em que pese essa definição possa não vir a ser sacramentada em um futuro próximo, ela já apresenta um grau de precisão e detalhamento que demonstra a flexibilidade necessária para a regulação de IA. Além disso, é importante destacar que, ao levar em consideração diversas técnicas, abordagens, atos e ações inerentes aos sistemas de IA,

essa definição consegue, de certa forma, promover a segurança jurídica que se espera.

Ultrapassado esse ponto conceitual, e ainda no que diz respeito à regulação de IA, foi apresentada a proposta europeia de definição do âmbito de aplicação de uma futura legislação específica. Como discutido anteriormente, esse também é um grande desafio a ser enfrentado pelos legisladores, uma vez que um eventual quadro regulamentar para a IA deve ser eficaz a ponto de atingir os seus objetivos, mas não demasiadamente prescritivo a ponto de criar um encargo desproporcional para o mercado. Nesse sentido, fica como desafio ao legislador buscar o devido equilíbrio entre proteger os direitos fundamentais das pessoas e, ao mesmo tempo, não promover uma restrição demasiada a ponto de impedir o desenvolvimento e a inovação no setor de IA.

Com esses requisitos em mente, foi também apresentada a proposta europeia de regulação de IA baseada em uma abordagem de risco, em que somente sistemas considerados de alto risco deveriam responder à uma legislação mais rigorosa. Para que isso ocorresse, tal proposta apresentou um método de classificação de sistemas de IA através de duas componentes, sendo elas o «setor» em que o sistema está inserido e o «uso pretendido» desse sistema. Dessa forma, para que um sistema seja considerado de «alto risco», ele deverá ser enquadrado concomitantemente nas duas componentes.

Além disso, é claro, também foi apresentada possíveis exceções a essa regra, na medida em que o uso pretendido de um sistema promove um risco tão elevado, que ele será classificado como de alto risco independente do setor que está inserido. Essas é uma proposta que foi ventilada no âmbito europeu e que, de certa forma, agrada por apresentar um encargo regulatório maior apenas para sistemas de IA que necessariamente promovem um elevado risco para indivíduos e para a sociedade. Isso permite, entre outras coisas, uma liberdade maior no desenvolvimento e na inovação de sistemas de IA que não representam tanto risco.

Assim sendo, após encerrar a apresentação das propostas europeias relacionadas à regulação de IA, fica-se na esperança de que, de alguma forma, esse conhecimento possa auxiliar o legislador brasileiro em seu desafio de trazer segurança jurídica e proteção de direitos fundamentais através de uma legislação brasileira para esse setor.

Referências Bibliográficas

CLARKE, R. Profiling: a hidden challenge to the regulation of data surveillance. Journal of Law and Information Science, Australia, v. 4, n. 2, December. 1993. Available at: http://www.austlii.edu.au/au/journals/JlLawInfoSci/1993/26.htmlD.

Ebers, Martin, Chapter 2: Regulating AI and Robotics: Ethical and Legal Challenges (April 17, 2019). Martin Ebers/Susana Navas Navarro (eds.), Algorithms and Law, Cambridge,

Cambridge University Press, 2019 (Forthcoming), Available at SSRN: https://ssrn.com/abstract=3392379 or http://dx.doi.org/10.2139/ssrn.3392379

European Data Protection Supervisor (EDPS), Opinion 3/2018 on online manipulation and personal data, March 19, 2018.

European Parliament. Artificial intelligence: From ethics to policy. EPRS | European Parliamentary Research Service. Scientific Foresight Unit (STOA). PE 641.507 – June 2020

Grupo de Peritos de Alto Nível em IA. Livro Branco sobre Inteligência Artificial: uma abordagem europeia de excelência e confiança.

Grupo de Peritos de Alto Nível em IA. Uma definição de ia: principais capacidades e disciplinas científicas

Magrani, Eduardo. Entre dados e robôs "Ética e privacidade na era da hiperconectividade". Publisher Arquipélago. 2019. ISBN 978-85-5450-029-0

Pasquale, Frank. The black box society: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015

E- COMMERCE

História do e-commerce: Como o surgimento da *World Wide Web* impactou no comércio

Lucas Cortizo[20]

Resumo:
Trata-se de artigo voltado a passar pelo conceito e história do e-commerce. Entender os impactos da internet sobre as relações comerciais e o surgimento de novas tecnologias faz-se necessário para vislumbrar o fenômeno do e-commerce. O texto busca mostrar que o comércio se mantém na sua essência, sendo atividade de compra, troca ou venda de mercadorias, produtos, valores, que entretanto vem sendo praticado também sob novas perspectivas, através de dispositivos informáticos que se comunicam através internet. Ademais, este artigo se propõe a contar os primórdios do e-commerce, sob a perspectiva da evolução da World Wide Web (WWW), que em paralelo viabilizou um ambiente propício à compra e venda na internet, alcançando o grande público de uma nova forma (através de aparelhos com acesso à WWW dentro do contexto doméstico). O leitor vai identificar que a forma gratuita de acessar o conteúdo online e em disponibilidade 24/7 estimulou a prática do comércio em ambiente digital, com o surgimento de plataformas notáveis que figuram atualmente entre as maiores empresas do mundo.

Palavras-chave: História do e-commerce; comércio eletrônico; desenvolvimento; internet; world wide web

---

[20] Advogado na Autoridade Nacional de Proteção de Dados do País de Malta; Representante de Malta na European Data Protection Board (EDPB) nos seguintes expert subgroups: International Transfers e Social Media; Representante de Malta na Global Privacy Assembly e na Common Thread Network; Participante da estratégia nacional de implementação da Inteligência Artificial em Malta; Especialista e Mestre em Direito e Tecnologia pela Universidade do Minho, Braga, Portugal; Graduado em Direito pela Universidade Federal de Pernambuco, Brasil; Coautor do livro União Europeia Interop 2019. Capítulo sobre Blockchain e e-Government, tendência da tecnologia na Administração pública; Fundador do Podcast "Direito Digital Cast"; Professor de Direito e Tecnologia em diversas instituições; Membro da European Artificial Intelligence Alliance, Bélgica.

Introdução

A invenção da internet na década de 1960 marcou uma verdadeira revolução da informação. Se nessa origem, a preocupação era meramente militar (a rede seria alternativa para hipótese de ataque inimigo nas redes de telecomunicações tradicionais), a rede ao se estabelecer, contou com a explosão de dispositivos informáticos domésticos, que ao chegar às residências das pessoas, aumentaram a velocidade e o volume das interações.

A internet ao chegar no mundo doméstico deu viabilidade a uma rede global, em que o mundo passou a interagir e gerar uma quantidade de dados jamais vista. A interação otimizou ainda mais com a chegada de dispositivos eletrônicos portáteis, que significou uma revolução dentro da própria revolução.

A partir do momento em que há um dispositivo qualquer, que pode ser carregado para todo lado, e acessado simultaneamente pela internet, o impacto não será apenas nas comunicações, mas em toda organização social. A comunicação eletrônica é um fenômeno humano. Por isso que se pode citar diversos fenômenos sociais que saíram além da prática tradicional e analógica, passaram a ser eletrônicos ou praticados de forma digital. Dentre eles, há um dos mais antigos institutos humanos: a troca voluntária de bens e serviços, mais conhecida como comércio.

A internet ofereceu, desta forma, uma tecnologia capaz de suportar um novo tipo de comércio, que surgiu em decorrência dela, o qual passou a ser chamado de e-commerce ou comércio eletrônico. No desenvolvimento dessa relação de causalidade entre a internet e o e-commerce, onde se consegue notar evidente que existe uma relação de consequência fundamental para um fenômeno que já existia desde os primórdios da civilização, nota-se uma interessante dicotomia: o comércio permanece o mesmo na essência (sendo a transação de compra e venda dos mais diversos itens), entretanto executado de uma forma completamente nova, através de dispositivos informáticos que se comunicam via internet.

Chega a ser interessante como o nível de comércio sempre foi fiel indicador do desenvolvimento de uma sociedade. Se as primeiras civilizações usavam trocas simples e escambo, foi a expansão do comércio que estimulou o contato transoceânico que moldou a geopolítica dos últimos séculos, nomeadamente do século XVI ao XX. No atual século, que já teve início no advento da rede mundial de computadores, o grau de engajamento das pessoas com sistemas de e-commerce parece indicar a que nível este grupo social está a se desenvolver.

Por tudo isso, discutir e debater formas de melhorar o e-commerce não significa apenas pensar em economia ou empresas, mas sim pensar também nos direitos fundamentais

dos consumidores, no incremento do sentimento de segurança e no desenvolvimento da sociedade.

1. Conceito do e-commerce

De acordo com o já explanado, o e-commerce é basicamente uma espécie ou forma de se executar o comércio eletronicamente, sendo uma via diferente da tradicional, na qual fornecedor e consumidor – em regra – estão presentes fisicamente em um mesmo ambiente (a exemplo de uma venda em estabelecimento comercial). Já é conceito que vem tentando ser definido por vários anos, e acaba por esbarrar na imensidão epistemológica dos termos envolvidos, o que conduz a uma verdadeira complexidade.

Por isso que a boa doutrina já reconhece esse desafio. Segundo PEREIRA , é complexo definir o comércio electrónico. Segundo uma noção puramente indicativa, trata-se da negociação realizada por via electrónica, isto é, através do processamento e transmissão eletrônicos de dados, incluindo texto, som e imagem.

Quando se estuda qualquer fenômeno que seja, é importante estudar a história do mesmo a fim de perceber sua origem e projetar seu futuro. Se o e-commerce de hoje se desenvolve a partir de plataformas em aplicações ou em websites, cuja prática se desenvolve através de uma loja virtual

onde com um simples clique confirmamos a compra feita baseada nos dados do cartão de crédito, todavia nem sempre foi assim.

2. Sistema de vendas à distância

Mais de um século previamente ao surgimento da internet, Richard Sears começou a desenvolver um sistema de vendas à distância através de catálogos, nos Estados Unidos no século XIX. Catalogando-se os produtos, com detalhes e fotos, ele conseguia vender em regiões remotas sem precisar ter lojas físicas ou nem mesmo o produto físico. A Sears, sua empresa, faturou bastante porque neste novo mercado, o fato da distância ajudava aos preços serem mais elevados. Existia pouca concorrência e o problema de logística permitia que vendas à distância apresentassem preços mais elevados.

O meio de comunicação que viabilizava esse comércio a distância embrionário era o telégrafo, sendo os produtos enviados por ferrovias. A melhoria dos meios de transporte potencializou principalmente a citada empresa pioneira, que em seu "Wish Book" já contava com mais de 700 páginas em produtos descritos e fotografados, sendo considerada a "Amazon do Século XIX" .

Então, nem mesmo o comércio a distância é alguma novidade, sendo a essência a mesma até hoje entre o catálogo

da Sears e a Amazon, por exemplo: lista-se produtos, com fotos, detalhes pormenorizados, preços e o consumidor irá declarar a vontade de comprar aquele produto. O comprador deverá fornecer algum meio seguro de pagamento, que o fornecedor verifique de maneira rápida a viabilidade de cobrança e em contrapartida o vendedor vai promover a logística de envio. Essa regra até o momento continua a mesma, o que mudou e sempre tende a mudar, são as formas de viabilizar essa dinâmica.

A implementação de uma tecnologia disruptiva tende a mudar as formas de executar a dinâmica das vendas descrita acima. E se podemos listar as grandes ideias da humanidade, sem dúvida o computador doméstico é uma delas. Na década de 1980, o computador pessoal chegou a um preço e tamanho que permitiu sua chegada às residências e pequenas empresas, e este movimento seria mais um fator importante para e-commerce. Dentre as grandes referências, merece destaque duas tecnologias que precederam a World Wide Web (WWW): o VideoTex e o Minitel.

3. Os frutos do *World Wide Web*

O Videotex era um sistema que fornecia aos usuários um acesso à informação em tempo real e de baixo custo para a época. Ele era basicamente um televisor modificado, com conexão à rede telefónica que permitia fazer compras online.

Pela imensa inovação à época, rapidamente espalhou-se e criou o fenômeno do teleshopping. Arriscando dizer que seria um verdadeiro ancestral do e-commerce. Aos parâmetros da época, tudo girava em torno de muita empolgação, notada na produção científica da época, que já estudava a arquitetura dos sistemas Videotex , na qual dava-se como pronto esse "novo modelo para entrega broadcast" que fora desenvolvido e a busca seria apenas melhorá-lo, como seu tempo de resposta.

Outro precursor do e-commerce, e quiçá da própria WWW atual, é o francês Minitel, que consistia em um terminal de texto conectado a uma linha telefônica que permitia realizar compras online, reservar passagens de trem, comprar ações na bolsa e etc. Interessante notar que a Mídia criou uma imensa barreira filosófica a essa tecnologia incipiente, porque se pensava que ela poderia ser utilizada para abusos, a exemplo de um sistema baseado no Minitel ou Videotex pudesse ser usado para propagandas governamentais. O que seria uma ameaça para o jornalismo escrito (curioso que atualmente a propaganda política online tem decidido eleições).

Há um detalhe a salientar-se que funcionou como grande vantagem para o Minitel alavancar de forma exponencial suas implementações. Detalhe este que foi verdadeiramente um elemento crítico para o sucesso do sistema, a saber o sistema de cobrança introduzido pela France Telecom em 1984, ao qual foi

dado o nome de Kiosk, através do qual as cobranças vinham na própria fatura com a denominação “Minitel use” .

Conforme o gráfico abaixo, pode-se perceber a evolução exponencial nos primeiros anos e uma queda abrupta de crescimento a partir da década de 90. Esse foi um verdadeiro sinal do que estava a se passar na época, uma vez que a tecnologia que revolucionou os anos 80 perdera espaço para uma nova ordem global, a World Wide Web (WWW).

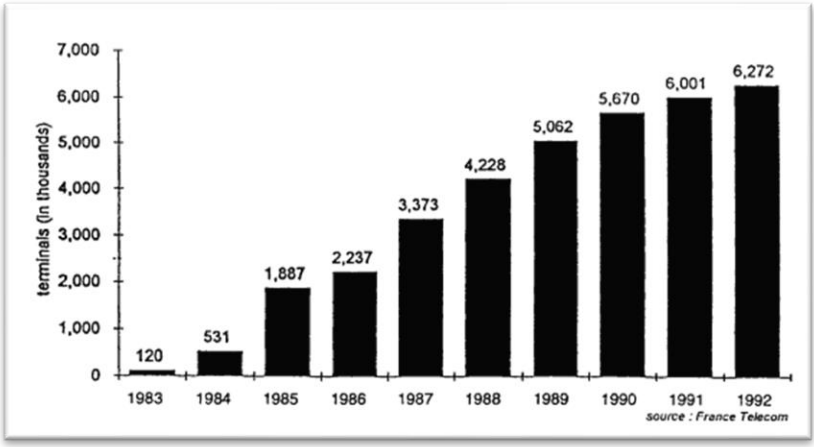

Figura 1 – Número de terminais Minitel[21]

Esta evolução da rede mundial de computadores mudou o mundo, e consequentemente o comércio. Se o Videotex e o

[21] Cats-Baril, William L., and Tawfik Jelassi. "The French videotex system Minitel...

Minitel faziam uma comunicação bilateral simultânea, a WWW tem dentre os segredos do seu sucesso a hiperligação unidirecional, o que acabou por viabilizar a criação de uma hiperligação sem qualquer ação do autor do documento a ser acessado, reduzindo de forma significativa a dificuldade de desenvolver um servidor Web e um navegador.

Ou seja, no aspecto do e-commerce, criou-se um ambiente perfeito para a oferta de produtos online de forma autônoma, em que o fornecedor não precisa estar em ligação direta e simultânea com o possível comprador, bastando fornecer dados necessários para que o consumidor por si só acesse através de um navegador próprio. Essa lógica de hiperligação unilateral da WWW foi fundamental para a criação de verdadeiras lojas online, totalmente automatizadas, e o melhor, abertas para compras 24 horas por dia e 7 dias por semana.

Essa abundância de abrangência e disponibilidade do e-commerce é reconhecidamente o segredo da sua expansão exponencial. É de se notar que estas características do e-commerce ultrapassam elementos que limitam a venda tradicional. Além dos fatores técnicos que permitem uma loja virtual 24/7, surgiu em 1994 um inovador meio de segurança na transferência eletrônica de dados que é o Secure Socket Layer (SSL), ou em outras palavras, um padrão global em tecnologia de segurança desenvolvida pela Netscape, cujo trunfo é criar um

canal entre o servidor web e um navegador (browser) para garantir que os dados sejam transferidos de forma sigilosa e segura .

Pode-se concluir, por hora, que, na Década de 1990, a WWW promoveu ruptura e inovação, sobretudo no e-commerce que já existia de outras formas como a Minitel ou Videotex. A inovação passa por dois pontos fundamentais: disponibilidade contínua de conteúdo e segurança das transações, afinal o formato de interação na WWW é através de navegadores (browsers) que tornam possível uma interatividade perene entre website-usuário, ou no presente caso fornecedor-consumidor, e ao mesmo tempo de forma segura e sigilosa, pela SSL ou pelo protocolo criptografado do HTTPS .

É notável como a questão das datas está tão presente na evolução histórica do e-commerce. Os formatos precursores - Videotex e Minitel - sofreram declínio a partir de 1993, mesmo ano em que é criado o Mosaic (navegador gráfico inovador). Ademais, a Organização Europeia de Pesquisa Nuclear anunciou que a WWW seria livre para todos, sem qualquer custo .

Não por acaso surgiu no ano de 1994 o SSL, e já no ano seguinte de 1995 são fundadas as maiores referências atuais de e-commerce: Ebay e Amazon. E essa mudança de paradigma, no contexto do surgimento de um estabelecimento de loja virtual através de um URL, um protocolo HTTP (em seguida evoluído ao HTTPS) que faz o protocolo de comunicação entre o servidor web

a qual essa loja virtual está vinculada e o navegador que receberá desse servidor o conteúdo em HTML - foi a nova dinâmica adotada pela atual fase do e-commerce.

Esses fatos históricos só mostram que a compra e venda sempre são institutos que não mudam em essência, apenas o que se altera são os processos e tecnologia envolvidos. A WWW viabilizou que a compra e venda na internet alcançasse o grande público e se transformasse em um fenômeno de massa. Tudo baseado em uma forma gratuita de acessar o conteúdo online, a qualquer momento ou horário, além de poder celebrar verdadeiros contratos, afinal os websites oferecem verdadeiras propostas contratuais prontas para serem celebrados com segurança e autenticidade.

E o movimento "lojas físicas vão virar lojas virtuais", ao contrário do que muitos previam para o futuro do e-commerce, nem chegou a ser hegemonia e desde sempre surgem diversos modelos de contratação. Um bastante famoso é o chamado online Marketplace, sobre o qual merece um detalhamento.

O conceito desenvolvido de Marketplace afasta o sentido de loja e cria mais um ambiente de feira. No e-commerce quem usa o domínio é simultaneamente a pessoa física ou jurídica que possui o bem a ser vendido, porém no online Marketplace, a plataforma providencia uma infraestrutura para vendedores e compradores conduzirem transações em um ambiente virtual . Essa definição aproxima o Ebay, da Olx, da Craigslist, do Silk

Road, dentre outras, sendo que cada uma dessas empresas ocupa um nicho de mercado com alguns pontos de convergência e concorrência. Em outras palavras, são verdadeiras plataformas em que uma terceira parte faz apenas o papel de oferecer otimizações e filtros de busca para facilitar que vendedor e potenciais compradores sejam conectados.

É interessante reparar que as plataformas de Marketplace oferecem um serviço básico gratuito, entretanto oferecem funcionalidades para potencializar o marketing do produto, sem qualquer garantia de que será vendido, e mesmo assim muitos fornecedores acabam pagando para potencializar sua publicidade dentro da plataforma, na aposta de obter mais alcance, e consequentemente mais produtos vendidos.

Um exemplo interessante é o mais popular Marketplace Sul-americano, fundado na Argentina em 1999, o Mercado Livre. O site/aplicativo permite compra de pacotes para melhorar o posicionamento nos motores de busca. Apesar de não cobrar para que o anúncio seja publicado, o valor da plataforma consiste em conferir autenticidade e níveis de reputação aos vendedores. Criou-se inclusive um método próprio de pagamento, denominado mercado pago, que o faz atuar como verdadeira instituição financeira online.

4. As gigantes do e-commerce

Tendo em vista que não existe um modelo único, seria relevante mencionar algumas das oito principais empresas de e-commerce para que se possa tentar notar diferenças entre elas.

I. A pioneira, a Amazon, funciona como um shopping online e apresenta o maior faturamento do mundo neste ramo.

II. Na China, há a gigante Jingdong que visa o mercado de entrega de sistemas, robôs, inteligência artificial e até drones.

III. De menor tamanho, se comparada com a anterior, mas de maior faturamento, há a Alibaba, que hoje já é famosa potência chinesa deste setor da economia.

IV. Outra pioneira já mencionada é o Ebay, que difere das outras por oferecer uma certa plataforma para leilões no Marketplace.

V. Significativamente se nota a japonesa Rakuten que funciona como um banco online e oferece sistema de cartão de crédito para pagamentos, além das vendas online.

VI. Merece também ser citada a B2W que é holding de diversos sites famosos de e-commerce na América Latina, como o Submarino e Americanas.com, fazendo com eficiência o modelo B2C dos mais diversos produtos.

VII. Na Europa, deve-se falar da Zalando que busca ser loja virtual para venda de artigos de moda.

VIII. E no fim desta lista, a Groupon que faz a venda de uma forma diferente, através da compra coletiva, na qual os usuários recebem descontos a cada meta de vendas atingida.

Listadas algumas das principais empresas de e-commerce do mundo, consegue-se aferir que empresas da Ásia conseguiram uma expressiva inserção nesta lista competitiva, outrora dominada pelos Estados Unidos. Ademais, que Europa e América do Sul apresentam pelo menos uma grande empresa nesse segmento de mercado, talvez necessitando adotar uma postura mais agressiva à luz das emergentes chinesas que conseguem escalar um mercado tão competitivo.

Considerações Finais

Uma vez mostrada a história do e-commerce, merece destaque notar que tudo passou a mudar muito mais rápido nos últimos anos. Ainda não sendo suficiente cravar projetos futuros, que prometem inovar mais ainda a forma de praticar o e-commerce, a lista das maiores empresas do ramo aparenta ser também uma lista de possíveis protagonistas para perspectivas futuras.

Apesar de tantas mudanças e quebras de paradigma, o fundamento continua o mesmo: práticas comerciais que envolvem múltiplas partes, que podem assumir a função geral de comprador e outras que assumem o papel de vendedor de bens e serviços. Se este processo acontece online, logicamente, muitas implicações surgem. A dinâmica muda naturalmente para se adaptar à disponibilidade total da internet, o que não quer dizer que a essência do comércio mude. Viu-se apenas uma das várias mudanças na forma que a humanidade pratica comércio e o desenvolvimento da tecnologia tem papel fundamental para tanto.

Na verdade, chega a ser um desenvolvimento recíproco, no qual a expectativa de mais lucro esperada por quem pratica comércio vai estimular o desenvolvimento de tecnologias para facilitar o mesmo comércio. E num investimento cíclico, o comércio ajuda no desenvolvimento de novas tecnologias e estas novas tecnologias vão desenvolver uma prática mais eficiente do próprio comércio. E nesta relação de reciprocidade, sem perder a essência, é onde se pode projetar os desdobramentos futuros do e-commerce.

Pensar no futuro deste novo comércio é evitar a limitação de que o atual e-commerce está perfeitamente acabado e segue imutável a curto e longo prazo. A própria economia, abrangendo relações de comércio, está em meio a um processo de reformulação, pois a cada dia o papel-moeda físico tem sido

modernizado por outras formas de pagamento, seja através do movimento online banking, seja pelas criptomoedas ou qualquer outra incorporação econômica de novas tecnologias.

Referências Bibliográficas

Berners-Lee, Tim. “Ten Years Public Domain for the original Web Software” 2003. Disponível em https://home.cern/resources/video/computing/message-tim-berners-lee-ten-years-public-domain-original-web-software. Acesso em 01/12/2018

Cats-Baril, William L., and Tawfik Jelassi. "The French videotex system Minitel: a successful implementation of a national information technology infrastructure." MiS Quarterly (1994): 1-20.

Christin, Nicolas. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace." Proceedings of the 22nd international conference on World Wide Web. ACM, 2013.

Carrijo, Leonardo. A história do Comércio Eletrônico. 2018. Disponível em http://www.vegasistemas.com.br/a-historia-do-comercio-eletronico/ Acesso em 14/11/2018

Girard, A. E. "The architecture of videotex systems." Electronics and Power 30.9 (1984): 733.

Pajovic, Stefan. Largest E-Commerce Companies in the World and No, Alibaba is Not the Largest Chinese E-Commerce. 2019. Disponível em https://axiomq.com/blog/8-largest-e-commerce-companies-in-the-world/

Pereira, Alexandre Libório Dias. Comércio eletrónico na sociedade da informação: da segurança técnica à confiança jurídica. Almedina, 1999.

Statista. Most popular online retailers in Latin America as of May 2018, based on number of unique visitors. 2018. Disponível em https://www.statista.com/statistics/321543/latin-america-online-retailer-visitors/

Wong, Johnny W., and Mostafa H. Ammar. "Analysis of broadcast delivery in a videotex system." IEEE Transactions on Computers 9 (1985): 863-866.

CRIMES INFORMÁTICOS

Breve historial da criminalidade informática e os riscos que representa para sociedade de informação

Abrantes Malaquias Belo Caiúve [22]

Resumo:
O galopante avanço da tecnologia informática trouxe muitos benefícios para a humanidade, dentre os quais destacamos o surgimento da Sociedade de Informação. Contudo, com este desenvolvimento surgiram igualmente alguns malefícios como o amplo incremento da criminalidade informática que afeta todo ciberespaço e coloca em risco a interconexão entre os cidadãos cibernéticos (netizens). Por isso, muitos países e organizações internacionais empenham-se na implementação de leis penais visando combater os delitos cibernéticos tendo como diploma modelo a Convenção de Budapeste do Conselho da Europa de 2001. Sendo assim, neste artigo apresentarmos uma resenha histórica que elucida a evolução histórica das infrações digitais, estudando a problemática que encerra a sua denominação e os perigos que apresenta na preservação da Sociedade de Informação.

PALAVRAS-CHAVE: Criminalidade Informática, Sociedade de Informação, Internet, Convenção de Budapeste, Ciberespaço.

[22] Licenciado em Matemática pela Universidade Agostinho Neto em Angola. Licenciado em Direito na opção Jurídico Forense no Instituto Superior Politécnico Jean Piaget de Benguela em Angola. Estudante do finalista da 8ª edição do Mestrado em Direito e Informática na Universidade do Minho em Portugal, tendo concluído o trabalho de dissertação com o tema "A problemática da regulação dos crimes informáticos no Anteprojeto de Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime" sob orientação dos professores Pedro Miguel Dias Venâncio e Joaquim Melo Henriques Macedo.

Introdução

Antes de entrarmos para as questões jurídicas faremos uma breve sinopse acerca do surgimento dos crimes informáticos.

Os registos dos primeiros casos de crimes informáticos remontam os meados da década de 60 e eram quase todos relacionados a crimes de imprensa ou económicos. Duas décadas depois começou a registar-se um aumento deste tipo de criminalidade que passou a envolver "manipulações de caixas bancários, abusos de telecomunicações, pirataria de programas e pornografia infantil"[23].

O desenvolvimento do comércio eletrónico possibilitou o surgimento de *sites* fraudulentos e de muitas burlas decorrentes do processo de compra e venda.

Deste modo, ficou evidenciado as vulnerabilidades que os sistemas nesse caso apresentavam, o que fomentou o surgimento das primeiras doutrinas sobre essa matéria[24].

Apesar dessas constatações delituosas, a palavra "cibercrime" surge apenas no final dos anos 90 em Lyon, França, no decorrer de uma reunião de um subgrupo do G8 que estudava e discutia os problemas que surgiam pelo uso das

[23] SANDRONI, Araújo Gabriela. Prevenção de Guerras Cibernéticas. IV Simpósio de Pós-Graduação em Relações Internacionais do Programa "San Tiago Dantas" (UNESP, UNICAMP e PUC/SP).
[24] **GOUVÊA**; Sandra. O direito na Era Digital. Crimes Praticados por Meio da Informática. MAUAD, Rio de Janeiro, 1997, p. 79.

redes de telecomunicações, numa altura em que se expandia o uso da internet, principalmente nos países do norte da América[25].

Em 23 de Novembro de 2001, esse termo foi incorporado no primeiro instrumento internacional sobre a temática, a *Convenção sobre o Cibercrime*[26] adotada em Budapeste, na Hungria pelo Conselho da Europa.

1. Breve evolução da criminalidade informática

Feita essa resenha histórica, começamos por frisar que os crimes informáticos em alguns aspetos assemelham-se aos crimes tradicionais, representando tão-somente "versões digitais no mundo real, ou seja, seriam crimes tradicionais se não fosse a adição do elemento virtual ou ciberespacial"[27].

O tratamento desse tipo de delito é tão recente e problemático que até a presente data não há unanimidade no

[25] Vale referir que a "introdução da interface gráfica ("WWW") deu-se igualmente nos anos 90, permitindo um rápido crescimento no número de usuários da Internet" e tornando a informação disponível globalmente. **GERCKE**, Marco. Understanding cybercrime: Phenomena, challenges and legal response. ITU (International Telecommunication Union). September, 2012. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (Acedido aos 28-01-2020).

[26] http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf (Acedido aos 02-03-2020).

[27] **MENEZES**, Umbelina Teresa João de. O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola. Dissertação para a obtenção do grau de Mestre em Segurança da Informação e Direito no Ciberespaço no Instituto Superior Técnico de Lisboa. Dezembro de 2016. https://fenix.tecnico.ulisboa.pt/downloadFile/563345090415229/Dissertacao.pdf (acedido aos 19-07-2019), p. 28.

que tange a sua designação, isto é, os crimes informáticos são igualmente designados por crimes virtuais, crimes digitais, crimes cibernéticos, crimes informático-digitais, e-crimes ou crimes eletrónicos[28].

Neste trabalho adotaremos a expressão "crimes informáticos" por ser aquela que se nos afigura mais abrangente.

Não existe uma definição única de crime informático[29] e a dificuldade dessa determinação tem várias razões, uma delas prende-se com o facto de que "os dados e sistemas informáticos tanto podem constituir objeto material de determinada conduta, bem como o instrumento utilizado para cometê-la"[30]. Outro motivo, se calhar o de maior realce, tem que ver com as "várias espécies de condutas humanas"[31] suscetíveis de representarem esse tipo de delito.

Crimes informáticos são aqueles orientados para o computador, ou seja, é um tipo de crime que pressupõe a existência de um computador e de uma rede. O computador

---

[28] As designações inglesas *high technology crimes* e *computer-related crime* são igualmente usadas por alguns autores lusófonos (in **DIAS**, Vera Marques. A problemática da investigação do cibercrime. **DATA VENIA - Revista Jurídica Digital.** Ano 1. N.º 01. Julho-Dezembro 2012, p.65).

[29] **MARQUES**, Garcia e **MARTINS**, Lourenço. Direito da Informática, 2ª ed., Almedina, p. 639.

[30] **DELGADO**, Vladimir Chaves. COOPERAÇÃO INTERNACIONAL EM MATÉRIA PENAL NA CONVENÇÃO SOBRE O CIBERCRIME. Dissertação apresentada como requisito parcial para conclusão do Programa de Mestrado em Direito das Relações Internacionais do Centro Universitário de Brasília, BRASÍLIA 2007, p. 18 e 19. https://repositorio.uniceub.br/jspui/bitstream/123456789/3562/3/vladimir.pdf (acedido aos 19-07-2019).

[31] **DELGADO**, Vladimir Chaves. Ibdem, idem, p. 19.

tanto pode ser utilizado para praticá-lo ou ser apenas o alvo de tal prática.

Nesta ordem de ideias, doutrinariamente os crimes informáticos podem ser definidos como "qualquer acção ilícita perpetrada com a ajuda de uma operação electrónica contra a segurança de um sistema informático ou de dados que ele contém, qualquer que seja o fim visado"[32].

Essa definição procura elencar a multiplicidade de ações que constituem esses delitos, porém não as discrimina na sua totalidade.

Este tipo de ilícito atenta, de modo particular, contra a própria pessoa ou contra a sua segurança financeira e, de modo geral, contra o bem-estar social.

Pode envolver ações que atentam contra os direitos autorais, a garantia dos direitos e liberdades fundamentais dos cidadãos (que é ferida pela vigilância massiva não autorizada), a extorsão sexual (também designada pelo neologismo *sextorsão*[33]), a pornografia infantil e outras más práticas.

A informática trouxe duas grandes problemáticas à legislação penal: serve como elemento potenciador da criminalidade e traz novas realidades que requerem a devida proteção legal.

---

[32] **RODRIGUES**, Benjamim Silva. Idem, p. 78, 79.

[33] https://www.jn.pt/justica/extorsao-sexual-na-net-nao-para-de-aumentar-4774319.html (acedido aos 03-11-2019).

A gravidade dos crimes digitais agudiza-se pelo facto de atentarem contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas informáticos.

Existem vários crimes informáticos e a sua nomenclatura altera de país para país, apesar de a maioria deles seguir a estabelecida na Convenção de Budapeste. Não é pretensão nossa elencarmos todos eles, contudo dentre os mais frequentes destacam-se a falsidade informática, o dano relativo a dados ou programas informáticos (ou simplesmente dano informático), a sabotagem informática, o acesso ilegítimo, a intercepção ilegítima, a reprodução ilegítima de programas de computador, a burla informática e a devassa por meio da informática.

Além da designação e da tipologia, outra temática isenta de unanimidade por parte dos distintos doutrinários é a relativa à sua classificação[34][35]. As designações mais frequentes são as seguintes: crimes informáticos próprios e impróprios[36]; crimes informáticos puros, mistos e comuns[37]; crimes informáticos em

[34] **RODRIGUES**, Benjamim Silva. Idem, p 19.

[35] A Comissão Europeia engloba no cibercrime três categorias de actividade criminosa, a saber, os **crimes tradicionais** cometidos com o auxílio do computador e redes informáticas, os **crimes relacionados com o conteúdo**, nomeadamente a publicação de conteúdos ilícitos por via de meios de comunicação electrónicos, e os **crimes exclusivos das redes electrónicas (DIAS**, Vera Marques. A problemática da investigação do cibercrime. **DATA VENIA - Revista Jurídica Digital.** Ano 1. N.º 01. Julho-Dezembro, 2012, p. 66).

[36] **CASTRO**, Carla Rodrigues Araújo de. Ibdem, p 230.

[37] **VIANNA**, Túlio & **MACHADO** Felipe. Crimes Informáticos. Belo Horizonte. Editora Fórum, 2013, p. 29-35. Nesta obra os crimes mistos são definidos como sendo "crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. São delitos derivados da invasão de dispositivo informático que ganharam *status* de crimes *sui generis*, dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos."
Para além da trilogia classificativa, os autores apresentam um quarto elemento de classificação que designam por *crime informático mediato ou indireto*, que sucede "nos casos

sentido amplo e em sentido estrito[38] e crimes de informática comum e específicos[39]. A primeira é a que nos confere melhor acolhimento.

Os crimes informáticos próprios ou puros são aqueles que só podem ser realizados fazendo recurso à informática, são tipos penais recentes, tendo surgido com o crescimento tecnológico. O bem jurídico tutelado é a inviolabilidade dos dados informáticos. Ou seja, "são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado[40]"

Já os crimes impróprios ou impuros surgiram porque a informática veio potenciar os delinquentes, por isso são crimes tradicionais cometidos por meio da informática, o que significa que são crimes comuns praticados na internet. Aqui o bem jurídico tutelado não é a inviolabilidade dos dados, mas sim outro.

---

em que um delito informático próprio é praticado como crime-meio para a realização de um crime-fim não informático". Como exemplo apresentam a seguinte situação: "Se alguém invade um dispositivo informático de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o de invasão de dispositivo informático e o furto; o primeiro, crime informático, o segundo, patrimonial.".

38 **VENÂNCIO,** Pedro Dias. Lei do Cibercrime Anotada e comentada. Coimbra Editora, Fevereiro de 2011, p. 17.

39 **ALBUQUERQUE**, Roberto Chacon de. A criminalidade informática. São Paulo, SP: Juarez de Oliveira, 2006, p. 241.

40 **JESUS**, Damásio E. de apud ARAS, Vladimir. Crimes de Informática. Jus Navigandi, Ed. 12, out. 2001. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. (Acedido em 03-11-2019).

No crime impróprio o resultado do delito repercute-se no meio natural, lesando o mundo físico ou causando ameaça a outros bens jurídicos não informáticos.

Nesta dupla classificação, a distinção fundamental reside no bem jurídico que se pretende tutelar, ou seja, os primeiros têm em consideração os crimes cometidos contra bens jurídicos informáticos e os segundos os cometidos contra bens jurídicos habituais.

A problemática do surgimento da criminalidade informática tem servido de impedimento à plena implementação e expansão da sociedade de informação e comunicação devido aos inúmeros riscos que causa, situação que examinaremos em seguir.

2. A sociedade da informação e os riscos que representa para a prática de crimes

A importância e a imprescindibilidade da internet são hodiernamente incontestáveis. A rede faz parte da vida das pessoas, sendo impossível resistir ao seu crescimento.

A internet trouxe muitas vantagens para diversas instituições tais como governos e empresas[41]. Contudo, apesar desses benefícios, a internet traz também consigo alguns

[41] As empresas "nela vêm uma excelente oportunidade de implementar e desenvolver os seus negócios à escala mundial". **RODRIGUES**, Benjamim Silva. Idem, p. 79.

malefícios tais como a perda da liberdade de expressão e informação como resultado da tentativa de controlo e da pressão exercida por parte de alguns regimes políticos.

Sendo assim, é impreterível analisar quais são os seus principais intervenientes e o respetivo grau da sua participação para o estabelecimento daquilo que se designa por "sociedade da informação".

Os Estados Unidos de América tiveram um papel preponderante na implementação da interligação da rede de computadores. Na primeira metade da década de 90 iniciaram um grande investimento na tecnologia como forma de potenciar o desenvolvimento económico e tal aposta possibilitou-lhes posicionar-se acima de outras nações incluindo o seu antigo rival que liderava o bloco do Leste.

As Nações Unidas também tiveram um papel de destaque. No início desse milénio surgiram várias resoluções e cimeiras ou cúpulas relacionadas às telecomunicações, à sociedade da informação e à governança na internet. Uma dessas cimeiras criou o *Grupo de Trabalho sobre o Governo na Internet* (GTGI)[42].

[42] Foi criado na cimeira de Genebra de 2003, de onde saíram dois grandes documentos: o Plano de Ação e a Declaração de Princípios. Dentre as Recomendações formuladas pelo GTGI destacam-se as que têm a ver com administração dos ficheiros da zona base e dos servidores base do sistema dos nomes de domínio; a atribuição de endereço IP; os custos de conexão; a estabilidade e segurança da internet e **ciberdelinquência**; a luta contra o *Spam*; a liberdade de expressão; participação efetiva na elaboração de políticas mundiais; a proteção dos dados e respeito pela vida privada; os direitos do consumidor e o multilinguismo. *Vide* **RODRIGUES**, Benjamim Silva. Idem, p. 80-85.

Foram traçadas diretrizes no sentido dos estados criarem um ambiente jurídico que propicie a implementação da sociedade de informação, visando o aproveitamento das suas potencialidades económicas[43].

É nesse clima que em 17 de maio de 2005 é instituído em Túnis – num encontro da Cúpula Mundial da Sociedade da Informação por via da Resolução 252 da 60ª sessão da Assembleia Geral das Nações Unidas – *o dia mundial da sociedade da informação.* Este grande feito visou despertar o mundo para a necessidade da luta pela redução da exclusão digital.

Seguindo a pretensão americana, a União Europeia em 1993 estabeleceu o caminho para uma "era comum de informação" como um dos seus desafios para o crescimento no século XXI[44].

---

[43] http://www.itu.int/net/wsis/implementation/index.html (Acedido aos 04-11-2019).

[44] Tal foi manifestado no **Livro Branco da Comissão Europeia** sobre o *Crescimento, competitividade, emprego. Desafios e pistas para entrar no século XXI quando* o eminente **Jacques Delors** era o presidente da Comissão Europeia. Neste documento oficial da União Europeia foi estabelecido um Plano de Ação que definiu as seguintes prioridades:
1ª Promover o uso das tecnologias da informação:
2ª Fornecer serviços básicos entre a Europa e resto do mundo;
3ª Continuar a criação do enquadramento jurídico apropriado;
4ª Apostar na formação nas novas tecnologias; e,
5ª Melhorar o desempenho industrial e tecnológico. Vide **RODRIGUES**, Benjamim Silva. Idem, p. 86-87.
Em 1999 na "cimeira do emprego" realizada em Lisboa e presidida por Portugal, o então primeiro-ministro **António Guterres** propôs que se transformasse "no lançamento de uma estratégia europeia para a sociedade do conhecimento". https://www.publico.pt/1999/12/03/jornal/uma-agenda-europeia-para-a-sociedade-do-conhecimento-127314, (Acedido aos 04-11-2019).

Em finais deste ano foi criado o Grupo de Alto Nível[45] liderado pelo alemão **Martin Bangemann** para analisar as transformações sociais relacionadas à Sociedade da Informação[46]. Era formado por especialistas seniores do setor europeu da informática, que refletiam sobre a necessidade do aumento da interoperabilidade de redes para simplificar a difusão de informações e sistemas de comunicação interativa.

Foi este grupo que preparou uma apresentação sobre o desenvolvimento da "sociedade da informação" na União Europeia para a Cúpula Europeia em Corfu, que decorreu de 24 a 25 de junho de 1994 e salientou a necessidade de criar um enquadramento legal, geral e flexível que estimule o desenvolvimento da sociedade da informação na Europa.

Estava assim lançada "a marcha para a sociedade da informação", surgindo em 1995 uma Diretiva[47] que definia pela primeira vez importantíssimos conceitos ligados à internet tais como: *dados pessoais, tratamento de dados e consentimento sem causa*. Nesse documento já foi notório o reconhecimento da não restrição ou proibição da "livre circulação de dados entre os Estados-membros".

---

[45] Um relatório desse grupo contendo inúmeras recomendações e intitulado ***Building the European information society for us all - Final policy report of the high-level expert group*** pode ser lido em http://aei.pitt.edu/8692/1/8692.pdf (acedido aos 04-11-2019).
[46] https://cordis.europa.eu/event/rcn/2139/es (Acedido aos 04-11-2019).
[47] **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046 (Acedido aos 05-11-2019).

Nos anos seguintes surgiram outros instrumentos normativos, todavia foi em 1999 que o Parlamento Europeu manifestou a urgência de ser fomentada "uma utilização mais segura da internet através do combate aos conteúdos ilegais e lesivos"[48] por intermédio da implementação de um plano de ação plurianual[49].

O novo milénio trouxe a inquietação relacionada com a "organização e gestão da internet"[50]. Seguiram-se preocupações concernentes aos "direitos do autor e conexos"[51] – bem como às "estatísticas comunitárias"[52] – tudo dentro da sociedade de informação.

---

[48] **Recomendação 98/560/CE do Conselho de 24 de Setembro de 1998 relativa ao desenvolvimento da competitividade da indústria europeia de serviços audiovisuais e de informação através da promoção de quadros nacionais conducentes a um nível comparável e eficaz de protecção dos menores e da dignidade humana.** https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:31998H0560 (Acedido aos 05-11-2019). Essas preocupações foram reiteradas anos depois pelo Comité das Regiões por via do parecer de 20 de Novembro de 2002.

[49] O documento orientador desse plano é a Decisão n° 276/1999/CE do Parlamento Europeu e do Conselho de 25 de Janeiro de 1999 que adopta um plano de acção comunitário plurianual para fomentar uma utilização mais segura da Internet através do combate aos conteúdos ilegais e lesivos nas redes mundiais.

[50] Resolução do Conselho de 3 de Outubro de 2000 relativa à organização e à gestão da Internet. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000Y1014(02)&from=EN (Acedido aos 05-11-2019). Na parte final dessa resolução pode que versa dobre a incumbência da Comissão pode ler-se o seguinte:
criar uma rede europeia que reúna as competências científicas, técnicas e jurídicas existentes nos Estados-Membros que se encontrem ligadas à gestão dos nomes de domínio, dos endereços e dos protocolos Internet.

[51] **Directiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação.** https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001L0029 (Acedido aos 05-11-2019).

[52] **Regulamento (CE) n.° 808/2004, de 21 de Abril de 2004, relativo às estatísticas comunitárias sobre a sociedade da informação.** https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32004R0808 (Acedido aos 05-11-2019).
Nessa matéria a estatística é muito importante porque permite tomar ações concretas e corrigir os problemas detetados.

A importância da adoção de instrumentos comunitários destinados a combater e sancionar *a criminalidade informática, a cibercriminalidade e a pornografia infantil* – reforçando a segurança no acesso à internet – ficou patente em 2001 na Comunicação da Comissão das Comunidades Europeias eEurope 2002[53]. No seu ponto 1.1. com a epígrafe *Respostas nacionais e internacionais,* lê-se a seguinte explanação interessante:

> "A criminalidade informática ou cibercrime afecta todo o ciberespaço e não pára nas fronteiras tradicionais dos Estados. Estas infracções podem, em princípio, ser cometidas a partir de qualquer ponto e contra qualquer utilizador de computador, independentemente do local onde se encontra. Reconhece-se de uma forma geral que se impõe uma acção eficaz, tanto a nível nacional como internacional, a fim de lutar contra a criminalidade informática".

[53] Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões - Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade - eEurope 2002 de 26.1.2001. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52000DC0890 (Acedido aos 05-11-2019).

É nesse clima que em novembro desse mesmo ano surge a Convenção de Budapeste sobre o Cibercrime já referida anteriormente e quatro anos depois a Decisão-Quadro 2005/222/JAI, de 24 de fevereiro relativa a ataques contra sistemas de informação[54].

Considerações finais

Apesar da ameaça que o cibercrime apresenta, reconhece-se que as tecnologias da informação, devido a facilidade de interação, geram maior produtividade e que a nova sociedade do conhecimento deve ser verdadeiramente inclusiva, e é por esse motivo que na Comunicação da Comissão ao Conselho – i2010[55] persistiu-se na tónica da construção de "um espaço europeu da informação" que responda à "convergência digital".

As preocupações com "a literacia e competência digitais, inovação e investigação, segurança e interoperabilidade digital,

[54] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=EN (Acedido aos 02-03-2020).

[55] Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões "i2010 – Uma sociedade da informação europeia para o crescimento e o emprego" de 1.6.2005. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PT:PDF (Acedido aos 05-11-2019).

Um ano antes era criada a Agência Europeia para a Segurança das Redes e da Informação (ENISA sigla em inglês) por via do **Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação**. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32004R0460 (Acedido aos 05-11-2019).

o mercado único digital e a qualidade de acesso à Internet[56]" foram levantadas em junho de 2010 quando foi aprovada a Agenda Digital, que substitui o programa eEurope, constituindo assim "uma das iniciativas-bandeira da Estratégia Europa 2020[57]".

De tudo que acima foi referido podemos notar que as tecnologias que motivaram o surgimento da sociedade de informação não são em si mesmo perniciosas, mas sim neutras. A sua periculosidade e os crimes que surgem nesses ambientes devem-se a sua má utilização.

Portanto, com o surgimento das redes sociais, torna-se necessário regular o seu uso e sancionar a utilização destas como meio de perpetração de ilicitudes ou como forma de facilitar o cometimento de infrações penais. Deste modo, urge realizar-se uma ampla campanha de formação dos usuários, porque só banindo a ignorância virtual teremos cidadãos menos suscetíveis aos ataques e maquinações dos criminosos cibernéticos.

Referências bibliográficas

ALBUQUERQUE, Roberto Chacon de. A criminalidade informática. São Paulo, SP: Juarez de Oliveira, 2006, p. 241.

[56] http://euroogle.com/dicionario.asp?definition=487 (Acedido aos 05-11-2019).
[57] Idem.

CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

DELGADO, Vladimir Chaves. COOPERAÇÃO INTERNACIONAL EM MATÉRIA PENAL NA CONVENÇÃO SOBRE O CIBERCRIME. Dissertação apresentada como requisito parcial para conclusão do Programa de Mestrado em Direito das Relações Internacionais do Centro Universitário de Brasília, BRASÍLIA 2007, p. 18 e 19. https://repositorio.uniceub.br/jspui/bitstream/123456789/3562/3/vladimir.pdf (acedido aos 19-07-2019).

DIAS, Vera Marques. A problemática da investigação do cibercrime. DATA VENIA - Revista Jurídica Digital. Ano 1. N.º 01. Julho-Dezembro 2012.

GERCKE, Marco. Understanding cybercrime: Phenomena, challenges and legal response. ITU (International Telecommunication Union). September, 2012. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (Acedido aos 28-01-2020).

GOUVÊA; Sandra. O direito na Era Digital. Crimes Praticados por Meio da Informática. MAUAD, Rio de Janeiro, 1997.

JESUS, Damásio E. de apud ARAS, Vladimir. Crimes de Informática. Jus Navigandi, Ed. 12, out. 2001. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. (Acedido em 03-11-2019).

MARQUES, Garcia e MARTINS, Lourenço. Direito da Informática, 2ª ed., Almedina, p. 639.

MENEZES, Umbelina Teresa João de. O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola. Dissertação para a obtenção do grau de Mestre em

Segurança da Informação e Direito no Ciberespaço no Instituto Superior Técnico de Lisboa. Dezembro de 2016. https://fenix.tecnico.ulisboa.pt/downloadFile/563345090415229/Dissertacao.pdf (acedido aos 19-07-2019).

VENÂNCIO, Pedro Dias. Lei do Cibercrime Anotada e comentada. Coimbra Editora, Fevereiro de 2011.

VIANNA, Túlio & MACHADO Felipe. Crimes Informáticos. Belo Horizonte. Editora Fórum, 2013.

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Compliance Digital: muito mais do que proteção de dados

Fernanda Galera Soler[58]

Resumo:
O objetivo deste trabalho é repassar o conceito de Compliance digital, o qual na atualidade não tem uma análise mais profunda e tampouco é amplamente estudado pela doutrina, existindo apenas noções de tal entendimento na prática jurídica. Igualmente, há o interesse em dissociar referido conceito das questões afeitas a proteção de dados, posto que este deve ser mais amplo do que apenas a conformidade a privacidade e as novas legislações sobre o tema.

Palavras-chave: Compliance Digital; Proteção de Dados; Direito Digital; LGPD.

[58] Aluna especial do Doutorado em Direito da Universidade São Paulo. Mestre em Direito Comercial, com foco em Propriedade Intelectual, pela Universidade São Paulo. Especialista em Propriedade Intelectual pela Escola Superior de Advocacia da Ordem dos Advogados do Brasil de São Paulo (2015). Graduada em Direito pela Faculdade de Direito de São Bernardo do Campo (2012). Advogada recomendada para o segmento de "Startups & Inovação - Escritórios de Advocacia", Leaders League. Advogada, professora da Direito FGV/SP e pesquisadora, com atuação nas áreas de Propriedade Intelectual, Inovação e Direito Digital. E-mail: fernandagalera@yahoo.com.br

Compliance Digital: muito mais do que proteção de dados

Um dos principais assuntos jurídicos dos últimos anos, amplamente debatido pela mídia, especializada ou não, é a questão da proteção dos dados pessoais e os desafios oriundos da adequação das suas normas pelos agentes do mercado. Com o advento da Internet, houve uma mudança no paradigma tecnológico, que mudou a forma como nos relacionamos, e até mesmo econômico[59], criando recentemente o debate sobre as formas de proteção do usuário neste ambiente digital e as problemáticas envolvendo a segurança das informações, gerando inúmeros debates acerca dos limites dos direitos atualmente existentes.

Diante destas mudanças sociais e tecnológicas, com um ajuda de inúmeros estudos realizado pela mais vasta gama de pesquisadores, inclusive juristas, o Brasil em 2014 criou o Marco Civil da Internet (Lei nº 12.965 de 2014) e recentemente a sua Lei Geral de Proteção de Dados, também conhecida como LGPD (Lei nº 13.709, de 14 de agosto de 2018), as quais conjuntamente com outras normas não tão conhecidas colocam o país na mesma sintonia legislativa dos países europeus .

Tais medidas buscam seguir a função e o interesse primígeno do Direito que é a adequação do homem à vida

[59] WERTHEIN, Jorge. *A sociedade da informação e seus desafios*. Ci. Inf., Brasília, v. 29, n. 2, p. 71-77, mai/ago 2000. Disponível em: < http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf >. Acedido a 15/03/2020.

social[60]. Sendo na atualidade este um grande desafio em razão do advento das novas tecnologias e da internet que causaram, juridicamente, dentre outros pontos: (i) a desumanização das relações; (ii) uma crise da expressão da vontade e do consentimento; (iii) a mudança das percepções do que é confiança e por vezes a sua exacerbação; (iv) reflexões acerca da quantidade e da qualidade da informação; (v) uma evolução galopante da tecnologia, que dificilmente é acompanhada por todos e que por vezes leva a erro muitas pessoas; (vi) o que causa uma dificuldade da apuração de riscos; sem falar da alteração do (v) tempo e (vii) espaço das relações.[61]

Diante deste cenário, parece que as relações humanas realmente mudaram com a transformação digital do mundo. Contudo, poucas áreas do Direito criaram conteúdos específicos e análises profundas sobre o tema. Ainda que exista um debate sobre a autonomia do Direito Digital[62] e suas mudanças, a doutrina majoritária ainda entende que existem apenas adaptações necessárias e mudanças para cada área em específico.

Dessa forma, o ambiente digital trouxe novos problemas, ampliando determinados Direitos e reativando certas questões, como é o caso da proteção de dados pessoais, a qual

---

[60] PEREIRA, Caio Mário da Silva. Instituições de Direito Civil, vol. I, 22ª edição, Rio de Janeiro: Ed. Forense, 2007.P. 07.
[61] CARBONI, Guilherme. Direito Digital Aplicado – Aula 1. Slides desenvolvidos para a apresentação a turma IV de Propriedade Intelectual e Novos Negócios da Direito FGV/SP.
[62] GUIMARÃES, Antônio Márcio da Cunha; GUIMARÃES, Gabriel. Direito Digital. Revista de Direito Internacional e Globalização Econômica. Vol 1, nº 2, jul-dez 2017, p. 70-81.

já existe um debate sobre a sua existência desde a década de 70[63] e diante da ampla utilização e possibilidade de tratamento de dados fornecida pelo avanço tecnológico agora está em voga.

Ocorre que para o jurista se inteirar da atualidade e efetivamente se alinhar a nova realidade digital não deve se passar somente por meio desta lei, mas há todo um arcabouço jurídico e legislativo[64] que permeia esse tema e vai além do texto

---

[63] MENDES, Laura Schertel. "A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis". In SOUZA; Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno especial: Lei Geral de Proteção de Dados (LGPD)*. 1ª edição, São Paulo: Thomson Reuters Brasil, 2019.

[64] As principais leis que permeiam o tema, posto que versam especificamente sobre o tema, ainda que sejam aplicáveis outras, como a Lei Anticorrupção Empresarial Brasileira (Lei nº 12.846 de 2013), podemos relacionar abaixo:

- Constituição Federal, especialmente na questão de princípios, direitos humanos e da criação do Habeas Data (Lei nº 9.507, de 12 de novembro de 1997);
- Código de Defesa do Consumidor (Lei nº 8.078 de 199);
- Lei nº 9.279 de 1996, versa sobre a proteção da propriedade industrial;
- Lei nº 9.609 de 1998, trata sobre a proteção do software.
- Lei nº 9.610 de 1998 dispõe sobre a proteção dos direitos autorais.
- Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), que tem como responsabilidade disciplinar a autenticidade, a integridade e a validade jurídica das assinaturas eletrônicas e demais assuntos relacionados as certificações digitais.
- Código Civil, como um todo! inclusive os artigos 225; 968, II e § 4º; 1180; e 1.358-Q, VIII – versam especificamente da realização de procedimentos e deveres de forma eletrônica.
- Lei do Cadastro Positivo (Lei nº 12.414 de 2011), disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.
- Decreto nº 9.936 de 2019, regulamenta a Lei do Cadastro Positivo.
- Lei de Acesso à Informação (Lei nº 12.527 de 2011), regula o acesso as informações sobre os órgãos públicos e de particulares em poder dos entes governamentais.
- Lei dos Crimes Cibernéticos (Lei nº 12.737 de 2012 - Lei Carolina Dieckmann), trata especificamente da realização de procedimentos e deveres de forma eletrônica.
- Decreto nº 7.962 de 2013, regulamenta o comercio eletrônico (e-commerce)
- Marco Civil da Internet (Lei nº 12.965 de 2014), estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- Decreto nº 8.771 de 2016, regulamenta o Marco Civil da Internet;
- Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018), dispõe sobre a proteção de dados pessoais.
- Decreto nº 10.046 de 2019, cria o Cadastro Base do Cidadão

da LGPD, posto que a realidade social seja no mundo físico, ou no digital, atua de forma mais ampla.

Dessa feita, até mesmo áreas mais atuais, como a de Compliance[65], precisaram se readequar a nova realidade social e implantar novas normas e estudos em seus trabalhos para que seja possível a efetiva proteção, mitigação de riscos e adequação a transformação digital a ampla utilização da Internet e as novas leis de proteção de dados.

Contudo, há de se entender o que seria o conceito de Compliance para esta nova sociedade, quais as medidas que devem ser tomadas, quais as preocupações existentes e do que versa especificamente esta área tão específica e nova do conhecimento jurídico, que recebeu o nome de Compliance Digital.

Para tanto, verificou-se que não existe uma ampla doutrina sobre o tema. Inclusive, existe uma certa dificuldade de encontrar um conceito para Compliance Digital em razão da sua novidade e atualidade, bem como, em atenção as mudanças

- Decreto nº 10.222, de 2020, aprova a Estratégia Nacional de Segurança Cibernética;
- Normas da "família" ISO 27.000, especialmente ISO/IEC 27000, ISO/IEC 27001 e ISO/IEC 27002. Tais normas trazem previsões acerca do Sistema de Gestão de Segurança da Informação, as quais versam sobre processos e procedimentos relacionados inclusive à segurança de dados e sistemas de armazenamento eletrônico.
- Além das normas setoriais, as internas das entidades, os contratos firmados, inclusive termos de uso e políticas de privacidade e a própria jurisprudência.

[65] Aqui não será realizado um estudo ou uma análise sobre a atualidade desta área, posto que apesar do dever de cumprir e agir de acordo com as normas existir há inúmeros anos. No Brasil esta área ganhou relevo e amplo destaque com a entrada em vigor da Lei Anticorrupção em 2013, sendo, por tal motivo, e apenas para fins do presente artigo considerada uma das novas áreas de estudo.

dos paradigmas educacionais que não fomentam a criação de estudos embasados e um aprofundamento jurídico sobre determinadas questões, mas sim experiências e conhecimentos práticos para soluções e aplicações imediatas, em razão da velocidade da evolução social e da liquidez de seus hábitos[66].

Por tal motivo, a busca de um conceito nacional focou na análise junto aos juristas especialistas sobre o tema, que ensinam e aplicam o Compliance Digital, conforme consta no site de suas práticas. Analisando o teor de suas publicações notamos que o conceito deste fica adstrito a uma questão central. Vejamos:

> "busca lidar com a atuação da empresa, bem como o tratamento dado às informações no ambiente digital. O propósito é assegurar que os processos internos e externos adotados pela organização no meio digital são compatíveis com as leis e regulamentações específicas desse ambiente."[67]

> "é a união entre a conformidade à lei e a tecnologia da informação para a gestão de riscos. E por riscos, incluímos aqui

[66] BAUMAN. Zygmunt. *A Cultura no Mundo Líquido Moderno*. 1ª Edição, Rio de Janeiro, Zahar, 2013.
[67] AMARAL, Rodrigo. *Compliance digital: o guia completo sobre o assunto*. Disponível em: < http://amaralmonteiro.com.br/compliance-digital-guia-completo/ > Acedido a 15/03/2020.

> uso indevido e vazamento de dados, invasão por malwares, phishings, propriedade de softwares, algoritmos e por aí vai."[68]
>
> "Compliance Digital, cuja função essencial é a análise de riscos e a adoção de medidas preventivas para adequação da empresa às regras aplicáveis às tecnologias da informação"[69]
>
> "O compliance digital, no âmbito empresarial, tem como principal função analisar os riscos e a adoção de medidas preventivas para a adequação da organização às regras aplicáveis às tecnologias da informação."[70]

Em leitura dos quatro conceitos trazidos por ilustres profissionais especializados sobre o tema, depreende-se que em todos há a relação entre o direito e a tecnologia da informação versando sobre questões pertinentes a internet e a proteção de dados. Na continuidade de tais publicações inclusive constam previsões especificas sobre tais pontos, com grande relevo à

---

[68] SARTORI, Adriana. *Compliance digital e LGPD: Tudo para seu escritório praticar*. Disponível em: < https://blog.sajadv.com.br/compliance-digital-e-lgpd/ > Acedido a 15/03/2020.

[69] *UGGERI, Karollyne. Compliance digital - os benefícios da implementação*. Disponível em: < https://www.migalhas.com.br/depeso/275349/compliance-digital-os-beneficios-da-implementacao > Acedido a 15/03/2020.

[70] LEC. JIMENE, Camilla. *Entenda Mais Sobre o Compliance Digital*. Disponível em: < https://lec.com.br/blog/entenda-mais-sobre-compliance-digital/ >. Acedido a 15/03/2020.

LGPD e muitas vezes um direcionamento quase que exclusivo as questões afeitas à privacidade.

É certo que o tema de debate do momento são as questões de privacidade, em especial após os escândalos envolvendo o vazamento de dados e a sua utilização[71]. Todavia, quando a expressão "Compliance Digital", há a aparência de maior amplitude do tema, ainda que para alguns este seja adstrito a tecnologia da informação. A última ainda é mais ampla do que a proteção de dados, existindo todo um arcabouço jurídico a ela ligado[72], bem como, uma série de questões técnicas dela derivadas.

Referido entendimento está em linha com as proposições da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[73] que dentre outras previsões recomenda que a transformação digital, inclusive no setor público, seja realizada por meio de integridade, transparência, inclusão e disponibilidade dos sistemas, incentivando a participação popular e com uma cultura analítica (direcionada por dados, sendo menos subjetiva[74]), mitigando riscos e evitando os problemas de segurança da informação e de privacidade, posto que estes são novos desafios trazidos.

---

[71] NETFLIX. Privacidade Hackeada.
[72] Vide nota de rodapé 6.
[73] OCDE. *Recommendation of the Council on Digital Government Strategies*. Disponível em: < https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/eventos/ocde/2017/workshop-com-luiz-de-mello-diretor-adjunto-de-governanca-publica-e-desenvolvimento-territorial-da-ocde/arquivos-sobre-governanca/4-recommendation-of-the-council-digital-government-strategies.pdf/view > Acedido a 15/03/2020.
[74] "Data driven culture".

Igualmente, deve ser fomentada a utilização de novas e/ou outras tecnologias, devidamente protegidas e liberadas, sendo garantida a sua entrada e participação pelos setores regulatórios para que seja possível uma efetiva e constante transformação digital.

Tais conceitos parecem mais amplos do que simplesmente o enfoque do compliance a tecnologia da informação. Passamos a análise de um caso existente para melhor verificar a construção do conceito em debate.

Analisando o modelo da Estônia[75] amplamente divulgado pela mídia como uma referência acerca de um país digital, ainda que seja discutível a aplicabilidade deste sistema no país, analisando as bases deste país notamos que estas vão muito além da proteção da privacidade e dos dados, posto que se baseia e três pilares: confidencialidade, integridade e disponibilidade.

O primeiro está intimamente ligado a proteção de dados, garantido a ampla informação daquilo que é necessário e nos limites do quanto desejado por cada um e para determinada finalidade. A disponibilidade trata do acesso as informações em um ambiente digital seguro e em pleno funcionando, o qual é confiável e que não prejudicará a realização de qualquer ato da vida humana.

---

[75] GUARDTIME. *Estonia Lessons Learned from a Digital Nation*. Slides criados para a apresentação ao Governo Federal em razão da meta de digitalização do Estado. Disponível em: < https://www.gov.br/secretariageral/pt-br/noticias/governo-federal-bate-meta-de-digitalizacao-anual/guardtime_brasilia_oct_19/view > Acedido a 15/03/2020.

Por fim temos a integridade, aqui vista como um dos pilares do Compliance que todo o sistema funciona de maneira ética e segundo as práticas pré-estabelecidas, mantendo assim a consistência e a precisão das informações, dados e processos, o que traz uma verdadeira segurança jurídica.

Analisando esses pontos temos que o desenvolvimento de uma sociedade digital vai além da proteção de dados e para a sua efetiva construção foi necessário também a construção de uma estrutura de segurança da informação e outros pormenores éticos e estruturais que somente são possíveis mediante a tomada de decisão e um processo de compliance no próprio país!

Outrossim, a experiência em comento consegue nos pontuar como é a experiencia real de adequação e cumprimento da transformação digital, por meio da mudança de uma sociedade como um todo para ser considerada efetivamente um país digital. Diante da dificuldade de encontrar um conceito sobre o tema, o entendimento deste caso em que houve uma ampla mudança do status quo ensina que apesar das questões relativas à proteção de dados serem pertinentes, há um universo além a ser entendido e aplicado efetivamente.

O caso da Estônia ainda detalha o pormenor acerca dos pilares sociais, os quais incluem a integridade, aqui em sentido amplo, posto que constituída como um pilar social, acredita-se que trata-se de uma análise para a construção do conceito de Compliance Digital, o qual passa por todos esses pontos e que é

uma das necessidades para a construção de qualquer entidade e sociedade.

Igualmente, as pontuações sobre a necessidade de cibersegurança, dever de auditar e reconciliar tecnologias e conhecimentos, com a existência de relação de confiança de terceiros são patamares pertinentes para a construção do que seria um Compliance Digital, os quais vão muito além do que trazido pela doutrina pátria.

Estudando a doutrina estrangeira, tampouco existe um conceito simples e definido do que é Compliance Digital, todavia, este é encontrado com uma explanação simples, porém, um pouco mais ampla do que as previamente destacadas, conforme recorte abaixo:

> "*the management of risks at the intersection of law, technology and the market that have emerged through and in reaction to the computerization and digital networking*"[76e77]

Os autores ainda destacam que que as áreas que se relacionam em primazia ao Compliance Digital, sem prejuízo de outras que existam ou que venham a existir, são privacidade, e

[76] "a gestão de riscos na interseção entre a lei, a tecnologia e o mercado que surgiram como uma reação à informatização e as redes digitais" (tradução nossa)

[77] GASSER, Urs; e HAEUSERMANN Daniel M. *E-Compliance: Towards A Roadmap for Effective Risk Management*. Disponível em: < https://scholar.harvard.edu/dhausermann/publications/e-compliance-towards-roadmap-effective-risk-management >. Acedido a 15/03/2020.

com ela as questões afeitas a proteção de dados e acesso à informação, segurança da informação, propriedade intelectual, direito do consumidor e governança do conteúdo.

Ao nosso entender, esse conjunto de normas está mais alinhados com as tratativas e previsões internacionais, a transformação digital e ao que o jurista deve analisar quando da sua preocupação com o Compliance Digital, posto que não se restringe a tecnologia da informação, mas se aplica a adequação e mitigação de riscos a todas as normas afetas a tecnologia, a Internet, ao ambiente digital e a atual Sociedade.

Outrossim, as áreas pontuadas por Gasser e Haeusermann[78] são mais amplas e mais certeiras quanto ao fenômeno vivido pela atualidade, posto que trazem as questões da proteção de dados em primeiro lugar inclusive, porém, também versam sobre as questões regulatórias e derivadas da tecnologia em si (segurança da informação e, em menor grau a propriedade intelectual).

Neste sentido, ao trazer ao debate a questão da governança do conteúdo, que pode atingir qualquer área do conhecimento, posto que deve ser observado o que está sendo criado, para qual finalidade, com qual direcionamento e com qual público. Cabendo aquele que busca se adequar as normas do ambiente digital analisar o sistema como um todo e não

[78] GASSER, Urs; e HAEUSERMANN Daniel M. *E-Compliance: Towards A Roadmap for Effective Risk Management*. Disponível em: < https://scholar.harvard.edu/dhausermann/publications/e-compliance-towards-roadmap-effective-risk-management >. Acedido a 15/03/2020.

apenas direcionado a questões relativas à proteção de dados ou segurança da informação.

Por todo o exposto e em linha com o quanto foi construído ao longo da presente exposição é que entendemos a necessidade de elaborarmos um conceito para Compliance Digital, de forma a começar a construir um estudo pátrio profundo que vá além da análise da LGPD, de questões pertinentes a proteção de dados ou mesmo da segurança da informação, mas que tal qual ocorre com o Direito Digital, ainda que não seja autônomo, precisa de um entendimento particular e mais amplo para a sua construção no país.

Outrossim, entendidos os conceitos que tratam o Compliance Digital como a adequação afeita as regras da tecnologia da informação, porém, diante da atual conjuntura social e da amplitude que tal área pode tomar é que é possível depreender que referida área é mais ampla do que referido conceito também.

Dessa feita, que em consonância com as reflexões trazidas ao longo da presente exposição é possível propor que Compliance Digital é a área do Direito, dentro das normas que versam sobre a conformidade das leis e normas internas e externas ("compliance"), analisa e estuda os fenômenos afetos ao ambiente digital, a tecnologia e a Sociedade da Informação.

Neste ponto temos então que o Compliance Digital permeia todos os meandros específicos trazidos por essa nova

realidade que trazida pelo século XXI, com a devida ampliação dos conceitos e estudos já realizados pela doutrina tradicional acerca das normas de Compliance.

Por tais motivos, as áreas que se relacionam em primazia ao Compliance Digital, sem prejuízo de outras que existam ou que venham a existir, são a privacidade, e com ela as questões afeitas a proteção de dados e acesso à informação, a segurança da informação, a propriedade intelectual, o direito do consumidor e a governança do conteúdo.

Referências bibliográficas

AMARAL, Rodrigo. *Compliance digital: o guia completo sobre o assunto*. Disponível em: < http://amaralmonteiro.com.br/compliance-digital-guia-completo/ >. Acedido a 15/03/2020.

BAUMAN. Zygmunt. *A Cultura no Mundo Líquido Moderno*. 1ª Edição, Rio de Janeiro, Zahar, 2013.

CARBONI, Guilherme. *Direito Digital Aplicado – Aula 1*. Slides desenvolvidos para a apresentação a turma IV de Propriedade Intelectual e Novos Negócios da Direito FGV/SP.

GASSER, Urs; e HAEUSERMANN Daniel M. *E-Compliance: Towards A Roadmap for Effective Risk Management*. Disponível em: < https://scholar.harvard.edu/dhausermann/publications/e-compliance-towards-roadmap-effective-risk-management >. Acedido a 15/03/2020.

GUARDTIME. *Estonia Lessons Learned from a Digital Nation*. Slides criados para a apresentação ao Governo Federal em razão

da meta de digitalização do Estado. Disponível em: < https://www.gov.br/secretariageral/pt-br/noticias/governo-federal-bate-meta-de-digitalizacao-anual/guardtime_brasilia_oct_19/view > Acedido a 15/03/2020.

GUIMARÃES, Antônio Márcio da Cunha; GUIMARÃES, Gabriel. Direito Digital. Revista de Direito Internacional e Globalização Econômica. Vol 1, nº 2, jul-dez 2017, p. 70-81.

LEC. JIMENE, Camilla. *Entenda Mais Sobre o Compliance Digital*. Disponível em: < https://lec.com.br/blog/entenda-mais-sobre-compliance-digital/ >. Acedido a 15/03/2020.

MENDES, Laura Schertel. "A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis". In SOUZA; Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno especial: Lei Geral de Proteção de Dados (LGPD)*. 1ª edição, São Paulo: Thomson Reuters Brasil, 2019.

NETFLIX. Privacidade Hackeada.

OCDE. *Recommendation of the Council on Digital Government Strategies*. Disponível em: < https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/eventos/ocde/2017/workshop-com-luiz-de-mello-diretor-adjunto-de-governanca-publica-e-desenvolvimento-territorial-da-ocde/arquivos-sobre-governanca/4-recommendation-of-the-council-digital-government-strategies.pdf/view > Acedido a 15/03/2020.

PEREIRA, Caio Mário da Silva. *Instituições de Direito Civil*, vol. I, 22ª edição, Rio de Janeiro: Ed. Forense, 2007.

SARTORI, Adriana. *Compliance digital e LGPD: Tudo para seu escritório praticar*. Disponível em: < https://blog.sajadv.com.br/compliance-digital-e-lgpd/ > Acedido a 15/03/2020.

SOUZA; Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). *Caderno especial: Lei Geral de Proteção de Dados (LGPD)*. 1ª edição, São Paulo: Thomson Reuters Brasil, 2019.

TAMER, Maurício Antonio; BUENO, Samara Schuch. "Compliance e aspectos práticos-legais da investigação em ambiente digital". In BECHARA, Fábio Ramazzini; Florêncio Filho, Marco Aurélio Pinto. *Compliance e Direito Penal Econômico*. São Paulo, Almedina, 2019.

UGGERI, Karollyne. *Compliance digital - os benefícios da implementação*. Disponível em: < https://www.migalhas.com.br/depeso/275349/compliance-digital-os-beneficios-da-implementacao > Acedido a 15/03/2020.

WERTHEIN, Jorge. *A sociedade da informação e seus desafios*. Ci. Inf., Brasília, v. 29, n. 2, p. 71-77, mai/ago 2000. Disponível em: < http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf >.

A Independência da Autoridade Nacional de Proteção de Dados e Comissão Nacional de Protecção de Dados a Luz da Constituição

Sircéia Macedo[79]

Resumo:
Quando falamos em Proteção de Dados, tanto no Brasil quanto em Portugal estamos falando de direito fundamental a luz da Constituição da República Federativa do Brasil de 1988 e da Constituição da República Portuguesa de 1976, respectivamente. Essa proteção Constitucional surge para expor a extrema importância dos dados pessoais que nas últimas décadas se transformaram em novos ativos onde fala-se em "Economia de Dados". Nesse sentido, a independência das autoridades designadas, nomeadamente, ANPD – Autoridade Nacional de Proteção de Dados e CNPD – Comissão Nacional de Proteção de Dados, se destaca em grande importância para a efetividade das normas.

Palavras-chave: Proteção de Dados; Economia de Dados; Independência; Vinculação; Tratamento de Dados; Dados Pessoais; Efetividade; Fiscalização; Privacidade; Direito Fundamental; Informação.

[79] Advogada no Brasil e em Portugal, Expertise em Estelionatos praticados por meio digital - *Web Developer* pelo Instituto Brasileiro de Pesquisa em Informática. Presença no Seminário de *Compliance* e Sustentabilidade Perspectiva Brasileira e Portuguesa na Universidade de Coimbra - Portugal, 2019. Mestranda em Segurança da Informação e Cibersegurança, Lisboa - Portugal. Pós-Graduanda em Advocacia Cível, UCAM, Brasil, 2019/2020. Capacitação em Direito Aéreo pela Associação Brasileira de Direito Aeronáutico e Aeroespacial - RJ, 2018. Capacitação em Procedimentos de Nacionalidade Portuguesa, Lisboa, 2018. Capacitação em Proteção de Dados - Lisboa, 2018, Curso de Capacitação 'Cidadão Ciberseguro', Lisboa, 2019.

Introdução

Apesar do destaque nos últimos anos no que se refere a proteção de dados, esse tópico está longe de ser uma novidade.

No ano de 1890, já se falava em Direito a Privacidade (The Right to Privacy, 1890).

Na Constituição da República Federativa do Brasil de 1988, inserido no título de Direitos e Garantias Fundamentais em seu artigo 5º, XII está a inviolabilidade e sigilo de dados, mas a Constituição da República Federativa do Brasil foi além e instituiu um remédio constitucional que assegura de forma específica a proteção dos dados, o Habeas Data, também inserido no artigo 5º e inciso LXXI, *in verbis*:

> *"LXXII - conceder-se-á habeas data:*
> *a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;*
> *b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"*

Em continuação, mesmo antes do Marco Civil da Internet instituído com a lei n.º 12.965 de 23 de abril de 2014, a proteção de dados já se efetivava com a utilização de leis esparsas como é o caso do Código de Defesa do Consumidor de 1990, Lei n.º

9.296 de 24 de julho de 1996 que trata das interceptações telefônicas, lei n.º 9.507 de 12 de novembro de 1997 que trata do direito de acesso a informações e disciplina o rito processual do habeas data, lei n.º 12.527 de 18 de novembro de 2011 que é a Lei de Acesso à Informação e o decreto n.º 7.962 de 15 de março de 2013 que regula a contratação no comércio eletrônico.

Atualmente no Brasil a Lei Geral de Proteção de Dados encontra-se em *vacatio legis*, com início de sua vigência prevista para agosto de 2020.

A Lei Geral de Proteção de Dados Pessoais, lei n.º 13.709 de 14 de agosto de 2018, foi inspirada no Regulamento (UE) 2016/679, que ocasionou um verdadeiro 'efeito dominó', visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a União Europeia, também deveriam ter uma legislação protetiva no mesmo nível do Regulamento (UE) 2016/679, (Pinheiro P. P., 2018).

Em Portugal, com o Regulamento (UE) 2016/679 - Regulamento Geral de Proteção de Dados, que foi diretamente aplicável a partir de 25 de maio de 2018, deixaram de existir 28 (vinte e oito) regimes harmonizados (Castro, O Regulamento Geral de Proteção de Dados Novos direitos e obrigações, 2018), para então ter-se um regime único sem prejuízo da legislação dos países membros.

Na Constituição da República Portuguesa de 1976 em seu artigo 26, n.º 1, há proteção a intimidade e a vida privada e

o artigo 35 tem grande destaque pois protege o direito à autodeterminação informativa, como também a independência administrativa da entidade que garante a proteção dos dados pessoais.

1. A proteção de dados pessoais como Direito Fundamental

Para se entender conceitualmente os Direitos Fundamentais, buscamos o ilustre doutrinador José Afonso da Silva que sintetiza: *"...designam prerrogativas e instituições que concretizam garantias de uma convivência digna, livre e igual de todas as pessoas e situações jurídicas sem as quais a pessoa humana não se realiza, não convive e às vezes, nem mesmo sobrevive, no sentido de que todos, por igual, devem ser não apenas formalmente reconhecidos mas concreta e materialmente efetivados ... Na expressão também se contém princípios que resumem uma concepção do mundo que orienta e informar a luta popular para a conquista definitiva da efetividade".* (Silva J. A., 2010)

Destaca-se a Carta dos Direitos Fundamentais da União Europeia em seu artigo 8º, que preconiza a proteção de dados pessoais como Direito Fundamental.

Nesse diapasão, o Regulamento (UE) 2016/679, logo em seu considerando 1 clarifica a proteção das pessoas singulares relativamente ao tratamento de dados pessoais como direito

fundamental. O considerando 4 do referido diploma esclarece que não se trata de um direito absoluto e deve ser mensurado com outros direitos fundamentais acordado a proporcionalidade.

No Brasil, em específico na Lei Geral de Proteção de Dados Pessoais – LGPD, preliminarmente em seu artigo 1, estabelece a proteção aos direitos fundamentais, *in verbis*:

> *Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.*

Ocorre que a Constituição da República Federativa do Brasil de 1988, não prevê a proteção de dados como Direito Fundamental, dessa feita em 2019, houve a iniciativa legislativa para a Proposta de Emenda Constitucional - PEC, 17/19, que prevê a inserção da proteção de dados na constituição, na lista de garantias individuais (Vital, 2019).

Não por acaso, os Direitos Fundamentais encontram-se positivados nas ordens jurídicas do Brasil e Portugal, essa internacionalização, se deve, também, a Carta da Organização

das Nações Unidas de 1945, que logo em seu início, preconiza os Direitos Fundamentais, *in verbis:*

> *Artigo 1. Os propósitos das Nações unidas são:*
> *3. Conseguir uma cooperação internacional para resolver os problemas internacionais de caráter econômico, social, cultural ou humanitário, e para promover e estimular o respeito aos direitos humanos e às liberdades fundamentais para todos, sem distinção de raça, sexo, língua ou religião.*

2. A independência aliada a eficiência a luz da constituição

Não obstante esperamos a luz dos direitos fundamentais constitucionalizados, dentre outros, uma postura negativa do Estado, com a independência temos uma aplicação apolítica, atemporal, proporcional, desierarquizada, igualitária e principalmente eficiente dos órgãos responsáveis pela proteção de dados.

Nesse sentido, a independência está aliada a eficiência pois consiste na ausência de subordinação em relação aos demais envolvidos, e tem como finalidade garantir uma atuação pautada estritamente pela convicção de seus representantes com relação as suas competências (Santos & Jr., 2012).

No parágrafo 3º do artigo 37 da Constituição da República Federativa do Brasil de 1988 e na Constituição da República Portuguesa de 1976 na alínea c) do artigo 81, preveem o princípio da eficiência, dessa forma, tem o Estado, dever constitucional de respeitá-lo.

Ocorre que, de nada adianta, a constitucionalização do referido princípio, ante a prática do Estado, ir na contramão dos deveres impostos, nesse sentido, nas palavras de Ivan Barbosa Rigolin:

> *"A inclusão do princípio da eficiência no texto constitucional foi a atitude mais ineficiente da vida dos autores da ideia, nos últimos 30 anos"* (Rigolin, 2003).

Aliado a independência, o ideal é a formação da tríade: eficiência, eficácia e efetividade, que por sua vez, não se confundem, pois, eficiência é o modo pelo qual se realiza – conduta dos agentes, eficácia é o meio e instrumentos empregados pelos agentes e a efetividade remete aos resultados obtidos (Filho, 2012).

3. A Autoridade Nacional de Proteção De Dados – ANPD (Brasil)

A criação da Autoridade Nacional de Proteção de Dados no regramento brasileiro inicialmente foi tentado no escopo da Lei Geral de Proteção de Dados Pessoais, que tendo em vista ser uma irregularidade técnica, foi iniciada a Medida Provisória 869/2018, de autoria do Poder Executivo, em 28/12/2018, tramitando em regime de urgência, por já ter sido colocado em vigência o Regulamento (UE) 2016/679, e que a referida medida provisória altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências [80].

A Medida Provisória, foi inaugurada, com nítida preocupação no que se refere a autonomia e independência da Autoridade Nacional de Proteção de Dados. Na Exposição de Motivos n.º 00239/2018 [81] logo em seu parágrafo terceiro, expõe que a "Autoridade Nacional de Proteção de Dados será criada como órgão da administração pública federal, integrante da Presidência da República", justificando a *suposta independência e autonomia* à natureza do mandato que somente será perdido por renúncia, trânsito em julgado de condenação judicial ou demissão decorrente de PAD (Processo administrativo disciplinar).

[80] https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190283
[81]https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1744791&filename=Tramitacao-MPV+869/2018

Ora, nítido a dependência vinculativa da Autoridade Nacional de Proteção de Dados ao poder público, vinculação essa, além de hierárquica, política, onde a natureza de sua função, que deve ter independência e autonomia plenos e não somente funcional, ficaram enclausuradas no próprio poderio Estatal, prejudicando desde sua forma inaugural, ou seja, desde a feitura legislativa, os resultados com ela pretendidos.

Em sequência, no Parecer n.º 1 de 2019 da comissão mista destinada a emitir parecer sobre a medida provisória n.º 869 de 28 de novembro de 2018 [82], na primeira audiência pública, a representante da Organização Coalizão Direitos da Rede, se manifestou com cabível preocupação quanto a compatibilidade da Autoridade Nacional de Proteção de Dados ao Regulamento (UE) 2016/679 no que diz respeito a necessidade de autonomia. Embora tenha se limitado a autonomia funcional, operacional, técnica e financeira e não plena, a qual englobaria toda e qualquer atribuição e competência, tal preocupação é cabível, visto a criação de um órgão completamente dependente e vinculado ao Estado, não alcança de forma alguma o êxito para qual foi criado.

No referido parecer, o Subchefe Adjunto Executivo da Subchefia para Assuntos Jurídicos da Casa Civil da Presidência da República, citou que "*em termos administrativos, ser*

[82]https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1745016&filename=Tramitacao-MPV+869/2018

integrante da Presidência é diferente de ser vinculado à mesma". Fica cristalino que do modo como foi criada, mesmo após o período transitório onde está previsto ser transformada em entidade da administração pública federal indireta, ficaria a escravidão da tutela administrativa, controle político, controle institucional, controle administrativo e controle financeiro.

O Ilustre Carvalho Filho, no Manual de Direito Administrativo (Filho, 2012), expõe: *"...pode afirmar-se que toda a pessoa integrante da Administração Indireta é Submetida a Controle pela Administração Direta da pessoa política que é vinculada*".

Caso não seja transformada em entidade da administração pública federal indireta, pois, de acordo com o parágrafo primeiro do artigo 55-A da lei n.º 13.853 de 8 de julho de 2019, ela "poderá" ser transformada pelo poder executivo, continuará a fazer parte da Administração Direta, cuja atividade é centralizada ao Estado e indissociável, grifo nosso:

> *"Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD),* ***órgão da administração pública federal, integrante da Presidência da República****.*
> *§ 1º A natureza jurídica da ANPD é* ***transitória e poderá ser transformada pelo Poder Executivo em entidade da administração***

> ***pública federal indireta, submetida a regime autárquico especial e <u>vinculada</u> à Presidência da República.***

Sobre a Autoridade Nacional de Proteção de Dados (ANPD) ser inaugurada como órgão da administração pública federal integrante da Presidência da República, tem-se o inciso I, do artigo 4º do decreto-lei n.º 200, de 25 de fevereiro de 1697, que expõe:

> *Art. 4° A Administração Federal compreende:*
> *I - A Administração Direta, que se constitui dos serviços integrados na estrutura administrativa da Presidência da República e dos Ministérios.*

A respeito da transformação para regime autárquico, é notório que a terminologia das autarquias tem o sentido de pessoa jurídica administrativa com relativa capacidade de gestão dos interesses a seu cargo, sob controle do Estado da qual originou. É uma parcela do próprio Estado. Quando o Estado cria autarquias visa descentralizar algumas funções. A função é meramente administrativa, por isso, a autonomia é o próprio Estado a autarquia é apenas uma pessoa administrativa criada pelo Estado. Tem personalidade jurídica de direito público, a cargo do Chefe do executivo fica sua criação e extinção em

respeito ao princípio da simetria das formas jurídicas (Filho, 2012), ainda no supracitado decreto-lei n.º 200, destaca-se o inciso I do artigo 5º:

> *Art. 5º Para os fins desta lei, considera-se:*
> *I - Autarquia - o serviço autônomo, criado por lei, com personalidade jurídica, patrimônio e receita próprios, para executar atividades típicas da Administração Pública, que requeiram, para seu melhor funcionamento, gestão administrativa e financeira descentralizada.*

Quando nos debruçamos especificamente no regime autárquico *especial,* a doutrina é direta no sentido de que a definição fica "duvidosa", abrangente e em aberto ao que deverá ser definido especificamente para o caso, inclusive quanto ao amparo constitucional que se deve ter. Trata-se de regime especial, ou seja, são atribuídos prerrogativas especiais e diferenciadas a essas autarquias, com peculiaridades e "regalias" (Filho, 2012).

Não obstante ao que seja definido após o período transitório, provavelmente ficará a cargo do Supremo Tribunal Federal uma definição definitiva, como aconteceu no caso do julgamento do Banco Central do Brasil na Ação Direta de Inconstitucionalidade n.º 449-2, DF, Sessão Plena, Relator

Ministro Carlos Velloso, Dj de 22.11.1996 [83], que, após ter a autarquia sido classificada como autarquia especial, teve o seu regime que ser definido definitivamente pelo STF.

Sintetizamos então a Autarquia de Regime Especial às prerrogativas: poder normativo técnico, autonomia decisória, independência administrativa e autonomia econômico-financeira (Madeira) (Filho, 2012).

As prerrogativas de certo que passam longe de serem absolutas e não podem deixar de submeter-se ao controle administrativo técnico. Não podemos esquecer que a competência para legislar no tocante a Proteção de Dados Pessoais será inserida na Constituição da República Federativa do Brasil e será exclusiva da União, por exemplo (Filho, 2012).

A autonomia decisória preconiza que os conflitos administrativos e inclusive a revisão destes, são dissolvidos no âmbito interno, sem prejuízo do direito constitucional do acesso à justiça. Como já exposto, por não serem prerrogativas absolutas, há entendimento que o poder revisional seja exercido pelos Ministérios, de ofício ou por provocação (recurso hierárquico improprio), quando ultrapassados os limites da competência ou contrariar políticas públicas do governo central (Filho, 2012).

A independência administrativa se dá por nomeação por tempo determinado, ocupam cargos em comissão, com a

[83] http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=266358

peculiaridade de ser a investidura por tempo certo. Para Carvalho Filho são "*agentes administrativos, alojados na categoria dos servidores públicos comuns de regime especial*" (Filho, 2012). Nesse sentido, o parágrafo primeiro dos artigos 55-D, 55-H e 55-I da lei n.º 13.853 de 8 de julho de 2019, expressa:

> *§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5.*
> *"Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal."*
> *"Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente."*

A autonomia econômico-financeira se dá por terem recursos próprios e dotações orçamentárias para gestão por seus próprios órgãos (Filho, 2012). Sobre esse ponto, importante que inicialmente a receita estaria vinculada a aplicação de multas e agora será destinado ao Fundo de Receita de Direitos

Difusos, como explicitado no parágrafo 5º do artigo 29º da Lei n.º 12.583 de 8 de julho de 2019:

> *§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.*

Fica notório a preocupação com a sintonia da legislação brasileira e da União Europeia, na terceira audiência pública do já referido parecer, onde o Ministro-Conselheiro da União Europeia no Brasil destacou a importância de uma autoridade independente, para que possa exercer suas competências sem qualquer influência política, ou seja, independência plena e não somente funcional.

Simplificado em uma frase a autonomia da Autoridade Nacional de Proteção de dados no artigo 55-B da lei n.º 13.709 de 14 de agosto de 2018:

> *"É assegurada autonomia técnica e decisória à ANPD".*

Em nenhuma parte da referida lei está previsto independência, também não poderia, pois está vinculado diretamente a Presidência da República.

Nesse sentido, a Proposta de Emenda à Constituição 17/2019 [84], prevê a inserção no corpo da Constituição da República Federativa do Brasil de 1988 a esperada independência, porém, na prática, não absoluta, por ser criada no berço de uma agencia reguladora pertencente a administração pública indireta, como está na proposta e abaixo elencado, grifo nosso:

> *Art. 21. Compete à União:*
> *XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei, que disporá sobre a criação de um órgão regulador independente."*
> *[...]*
> *Art. 4º Para os efeitos do inciso XXVI do art. 21, na redação dada pelo art. 2º desta Emenda, o órgão regulador será entidade* ***independente, integrante da administração pública federal indireta, submetida a regime autárquico especial****.*

4. A Comissão Nacional De Protecção de Dados – CNPD (União Europeia e Portugal)

[84] https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1844229&filename=Parecer-PEC01719-10-12-2019

Importante destacar inicialmente que quando falamos em Autoridade de Controle, estamos falando no âmbito da União Europeia e Comissão Nacional de Proteção de Dados, no âmbito de Portugal e/ou Estados-membros.

Em 1994, o nº 1 do artigo 4º da Lei nº 10/91 de 29 de abril, cria e define as atribuições da Comissão Nacional de Protecção de Dados Pessoais Informatizados (CNPDPI).

Em seguida no nº 2 do artigo 4º da Lei nº 10/91 de 29 de abril, em consonância com a Constituição da República Portuguesa, na revisão constitucional de 1997, é delineado que a autoridade é uma entidade pública e independente, (Castro, e-Pública: Revista Eletrónica de Direito Público, 2016).

Ora, não ter interferências político-administrativas na máquina pública, atuando com total independência se faz primordial para o início de uma atividade de extrema importância para a nação que inclui também, diversas jurisdições, como é conhecido no Mercado Único Digital[85].

Os artigos 22 e 23 da Lei n.º 67/98 de 26 de outubro[86] expressam as atribuições e competências da Comissão Nacional de Protecção de dados, fato que para fiscalizar, investigar, ordenar bloqueios, apagamentos, advertir, censurar, intervir em processos judiciais e principalmente deliberar sobre a aplicação

[85] [85] https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0228&from=EN
[86] https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm

de coimas, deve ser completamente independente pois, atua também, no âmbito público além do privado.

A regulação veio com a Lei n.º 43/2004, de 18 de agosto [87], repisando a independência da entidade.

O Regulamento (UE) 2016/679, em seu artigo 51 ratifica a independência das autoridades de controle, que devem existir em todos os estados-membros, lembrando que a figura já era prevista, como supracitado, no artigo 28º da Diretiva 95/46/CE e no artigo 21 da lei n.º 67/98, de 26 de outubro (Pinheiro, Coelho, Duarte, Golçalves, & Gonçalves, 2018).

Para o Ilustre Alexandre Souza Pinheiro [88]: *"...beneficia do distanciamento em relação às conjunturais maiorias parlamentares ou a titularidade do poder executivo...Libertas da direção, tutela ou superintendência do poder político...a decisão técnica supera, em ganho para o bem comum, a opção política".*

Ora, o objetivo é a não integração a administração direta do estado, nem a indireta que de qualquer forma, apesar de descentralizada, está ligada pelo princípio da vinculação a administração direta. Os interesses não podem emergir dos poderes do estado, devem ser autônomos e independentes sem qualquer interferência política para a realização da atividade técnica-administrativa da Comissão Nacional de Proteção de

[87] https://dre.pt/pesquisa/-/search/480712/details/maximized
[88] Alexandre Souza Pinheiro, "Privacy e Proteção de Dados Pessoais: A Construção Dogmática do Direito a Identidade Internacional", cit., p. 732.

Dados, sob pena de ter todas as suas atribuições e competências comprometidas.

O considerando 117 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), de extrema importância para elucidar as questões posteriormente deliberadas por cada estado-membro, inclusive sendo vinculativas em decisões judiciais, expressa (grifo nosso):

> *"**A criação de autoridades de controlo nos Estados-Membros, habilitadas a desempenhar as suas funções e a exercer os seus poderes com <u>total independência</u>, constitui um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais.**"*

Ressalta-se que, quando da feitura da legislação interna dos estados-membros, devem observar a exatidão do "total independência" deliberada no referido Regulamento (UE)

2016/679, não se limitando a uma mera independência funcional no âmbito de um setor não público [89] .

Não pode de certo, pois vai de contra ao preconizado no referido Regulamento (UE) 2016/679, atribuir outra roupagem, a possíveis influências do Estado às autoridades de controle, como por exemplo, por instruções externas, nem mesmo a solicitarem, bem como por aconselhamentos externos (Pinheiro, Coelho, Duarte, Golçalves, & Gonçalves, 2018).

O que não deve se confundir como ausência de independência é a necessidade de liberação de recursos financeiros dados as autoridades de controle, e ainda completa o considerando 120 do Regulamento (UE) 2016/679: "*As autoridades de controlo deverão ter orçamentos anuais públicos separados, que poderão estar integrados no orçamento geral do Estado ou nacional*".

Não obstante, na Lei n.º 58/2019 de 8 de agosto [90], Lei de Execução do Regulamento (UE) 2016/679 em Portugal, no número 1 do artigo 4º, repisa a independência harmonizando o preconizado no referido regulamento:

> *"1 - A CNPD é uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de*

[89] https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62007CJ0518&from=PT
[90] https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized

autonomia administrativa e financeira, que funciona junto da Assembleia da República."

Considerações finais

Para alcançar o objetivo fundamental que é a proteção dos dados pessoais a independência total da autoridade de controle é primordial.

A legislação brasileira foi inspirada e realizada com foco na legislação europeia, em específico no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Por óbvio a estrutura dos poderes, entre Brasil e Portugal são distintas, o Regulamento é diretamente aplicável, porém é pendente de uma lei de execução que por sua vez é elaborada pelos respectivos Estados-membros em suas jurisdições.

Dessa feita, ao se inspirar no modelo Europeu, não se preocupou com as peculiaridades da República Federativa do Brasil, extensão territorial dentre, principalmente no que se refere a Autoridade Nacional de Proteção de Dados Pessoais.

A proteção constitucional levada pela Constituição da República Portuguesa no número 2 do artigo 35 é replicada no

supracitado regulamento bem como na legislação de execução, isso leva a uma garantia constitucional de cumprimento da independência e autonomia total da Comissão Nacional de Protecção de Dados, no caso de Portugal.

O referido regulamento europeu também prevê, caso haja necessidade, a previsão na ordem interna dos Estados-membros de mais de uma autoridade de controle, ou seja, com o intuito de levar eficiência prática esperada pela proteção de dados.

De outro lado, no Brasil, a criação de apenas uma autoridade de controle já levou a grandes impasses políticos, técnicos e legislativos, e com elucidado, longe de ser uma autoridade independente.

Devido a entrada em vigor do regulamento europeu, o Brasil passou por um verdadeiro processo célere para aprovação de uma legislação de proteção de dados, que teria o objetivo de ficar no nível da proteção europeia para que as relações comerciais continuassem sem o risco de qualquer incidente relacionado a proteção de dados.

A independência esperada e não conquistada na legislação brasileira, que está prevista para entrar em vigor em agosto de 2020 ainda terá diversos desdobramentos, primeiro por ser inaugurada sem qualquer independência, ligada diretamente à Presidência da República, segundo por ter previsão transitória e previsão de transformação em autarquia especial, que para a doutrina e na prática, é uma criação com

peculiaridades imprevisíveis – regalias, o que poderá e provavelmente deverá ficar a cargo do Supremo Tribunal Federal para uma definição definitiva.

De certo que uma independência relativa está distante de ser uma independência total, como no caso da legislação europeia. Essa independência relativa é a que está em aprovação na Proposta a Emenda Constitucional 17/2019.

Referências bibliográficas

Brasil, B. C. (2020, Janeiro 02). Relatório de Estabilidade Financeira de Outubro de 2019. Tratto da BCB.GOV.BR: https://www.bcb.gov.br/content/publicacoes/ref/201910/RELESTAB201910-refPub.pdfáficas

Castro, C. S. (2016, Dezembro). e-Pública: Revista Eletrónica de Direito Público. Tratto da 40 anos de "Utilização da Informática" - O artigo 35.º da Constituição da República Portuguesa: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2183-184X2016000300004

Castro, C. S. (2018). O Regulamento Geral de Proteção de Dados Novos direitos e obrigações. Lisboa, Portugal.

Filho, J. d. (2012). Manual de Direito Administrativo. Atlas S.A.

Madeira, J. M. (s.d.). Administração Pública.

Pinheiro, A. d., Coelho, C. P., Duarte, T., Golçalves, C. J., & Gonçalves, C. P. (2018). Comentário ao Regulamento Geral de Proteção de Dados. Lisboa: Almedina.

Pinheiro, P. P. (2018). Proteção de Dados Pessoais Comentários à Lei n.º 13.709/2018. Saraiva Jur.

Rigolin, I. B. (2003). O servidor público nas reformas constitucionais. Fórum, p. 26.

Santos, R. F., & Jr., V. M. (2012). Constituição Federal Interpretada. Manole.

Silva, J. A. (2010). Curso de Direito Constitucional Positivo. Malheiros Editores.

The Right to Privacy. (1890, Dezembro 15). Tratto da Cornell CIS Computer Science: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Vital, A. (2019, Dezembro 10). Camara dos Deputados. Tratto da Camara dos Deputados: https://www.camara.leg.br/noticias/624541-COMISSAO-APROVA-PROPOSTA-QUE-INSERE-PROTECAO-DE-DADOS-PESSOAIS-NA-CONSTITUICAO

STARTUP

A evolução do Vesting

Lucas Prado[91]

Resumo:
Propõe-se aqui investigar as origens do vesting para refletir com clareza sobre as tendências desse tipo de contrato para o futuro. Apesar da sua natureza jurídica controversa e de sua incompatibilidade com alguns ordenamentos jurídicos, o vesting é um fato jurídico, sendo adotado principalmente por startups em todo o mundo. Portanto, o foco será primordialmente histórico e evolutivo, ponderando sobre os riscos e os resultados observados em relação ao contrato de vesting. Não há dúvidas de que este tipo de contrato foi uma inovação jurídica que trouxe grandes benefícios no sentido de alinhar os interesses dos fundadores, funcionários e investidores, com os objetivos chave da empresa. Por essas e outras razões, o vesting se tornou um modismo, mas, como toda moda passa, é importante observar os processos de adaptação desse tipo de contrato às mutações do mundo do trabalho.

Palavras-chave: startup; investimento; direito contratual; inovação; govtech

[91] Servidor público da Justiça do Trabalho, bacharel em direito pela UFV, especialista em Direito do Trabalho pela Faculdade Damásio e Co-Founder da Meryt, uma govtech de people analytics. Mora em Manaus onde atua ativamente no ecossistema de startups como catalisador de inovação e entusiasta de dados abertos. Além disso, escreve artigos como colaborador para diversos sites como o JOTA, LeMonde Diplomatique e Justificando. Foi um dos idealizadores da FreeLaw, lawtech que ficou em 3º lugar no primeiro Global Legal Hackhathon. Já participou da organização de grandes eventos como o AmazonHackfest, VHSummit Governo e Tecnologia e o Govtech Connection e foi palestrante na Campus Party Digital Amazonas 2020

Introdução

Os contratos de *vesting* se espalharam pelo mundo rapidamente. Muito utilizados nos ecossistemas de *startups,* como no Vale do Silício, por exemplo. Segundo o *National Center for Employee Ownership*[92] o número de trabalhadores vestados nos Estados Unidos aumentou nove vezes desde o final dos anos 80.

Estima-se, com base no último levantamento feito em 2016, que existam aproximadamente cerca de 14,2 milhões de funcionários participantes de planos de opção de compra de ações, dos quais o *vesting* vem se tornando uma das modalidades mais adotadas. Em 1993, cerca de 20% da remuneração dos executivos era baseada em ações, de acordo com Lynn Stout, da *Cornell Law School*[93]. Hoje, o patrimônio representa cerca de 60% da remuneração dos executivos das empresas do índice de ações Standard&Poor's500.

Buscando-se compreender a razão desse crescimento acelerado é possível supor que exista um grande valor nesse tipo de contrato. Olhando para a maioria das *startups* podemos perceber que a grande parte delas inicia suas operações sem capital ou com muito pouco capital, o que dificulta em grande medida a contratação de funcionários. De tal forma que o *vesting*

[92] https://www.investopedia.com/managing-wealth/get-most-out-employee-stock-options/

[93] https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2310&context=facpub

se tornou uma solução atrativa para ambas as partes. De um lado funcionários dispostos a dividir os riscos do negócio, investindo seu tempo e mão de obra numa aposta, e de outros sócios em busca de um "*dream team*" para fazer seus negócios decolarem.

Por essas razões, o contrato de vesting disseminou-se no ecossistema empreendedor como uma forma de reter talentos e promover incentivos em um momento crucial da *startup*, quando ela opera em *bootstrapping*. Olhando assim, o *vesting* parece ser a solução perfeita! Contudo, tal instituto jurídico quando não é bem utilizado, pode causar mais problemas do que soluções, uma vez que em uma startup tudo está sempre em transformação, o que cria um ambiente de negócios repleto de incertezas. O que muitas vezes parece um sonho, pode acabar se tornando um pesadelo.

Startup é uma expressão geralmente utilizada para se referir a sociedades iniciantes no mercado, muitas delas sem registro formal de pessoa jurídica, mas com ideias inovadoras em determinado ramo ou atividade econômica, dispostas a desenvolver um novo modelo de negócio que seja repetível e escalável[94]. Uma *startup* é, portanto, "*a human institution designed to create a new product or service under conditions of extreme uncertainty*" (RIES, 2011, p. 37), ou seja, um

[94] BLANK, Steven. The startup owner's manual: The step-by-step guide for building a great company. John Wiley & Sons, 2020.

empreendimento criado por pessoas para desenvolver um produto/serviço inovador em circunstâncias de extrema incerteza.

O sucesso de uma sociedade que adota o modelo de *startup* está normalmente relacionado com a sua capacidade de inovação, o que poderá significar um possível crescimento futuro. Porém, nesse contexto de inegável incerteza e riscos, é comum que surjam relações tensas e divergentes, sendo o conflito entre os sócios o principal fator de fechamento das *startups* brasileiras[95]. Assim, acordos e contratos se tornam necessários no sentido de solucionar e evitar os conflitos, protegendo direitos e garantindo segurança jurídica.

Uma das características do modelo de *startups* é também a alocação de capital de incentivo aos membros da equipe. Compartilhar a vantagem com a equipe pode ser uma ótima maneira de criar o espírito de equipe, reduzir as despesas de compensação em dinheiro e incentivar os funcionários a permanecerem à medida que a *startup* cresce. Visando alinhar os interesses dos fundadores, funcionários e investidores, com os objetivos chave da empresa surgiram as "*employee stock options*", dando aos funcionários o direito, mas não a obrigação, de comprar um ativo em uma data futura, por um preço previamente estabelecido. Segundo Andy Rachleff, fundador da

[95]https://epocanegocios.globo.com/Empreendedorismo/noticia/2016/07/74-das-startups-brasileiras-fecham-apos-cinco-anos-diz-estudo.html

Wealthfront, alguns dos benefícios das opções de ações são que "alinham o risco e a recompensa dos funcionários que apostam em uma empresa não comprovada, recompensam a criação de valor a longo prazo e pensam pelos funcionários, e incentivam os funcionários a pensar sobre o sucesso holístico da empresa."[96]

Isso pode ser algo bastante vantajoso do ponto de vista de um empregado que esteja disposto a correr riscos. Um exemplo famoso de alguém que fez essa aposta e obteve grande sucesso é o do artista David Choe. Ele pintou murais nas paredes do escritório original do Facebook em Palo Alto, Califórnia. O Facebook, era uma *startup* de apenas um ano da época e ofereceu a ele uma escolha entre um pagamento de vários milhares de dólares ou algumas ações do Facebook que tinham o mesmo valor (na época). Embora, Choe não tivesse muita expectativa no futuro do Facebook, ele preferiu apostar e pegou as ações em vez do dinheiro e as segurou. Em 2012, às vésperas da oferta pública inicial de ações (IPO) do Facebook, ele faturou US$ 200 milhões com a venda das ações[97].

No Brasil este tipo de contrato de *vesting* tem se tornado bastante popular, apesar das controvérsias a respeito da melhor forma de utilizá-lo, uma vez que não há previsão desse tipo de contrato no ordenamento jurídico pátrio, sendo caracterizado

[96] https://firstround.com/review/The-Right-Way-to-Grant-Equity-to-Your-Employees/
[97]http://epocanegocios.globo.com/Revista/Common/0,,EMI292604-16418,00-GRAFITEIRO+VAI+LEVAR+US+MILHOES+COM+IPO+DO+FACEBOOK.html

como contrato atípico nos termos do art. 425, do Código Civil Brasileiro. Cabe salientar, que embora permitida a utilização do *vesting*, o tipo societário mais afeto à este contrato, seriam às sociedades por ações, reguladas pela Lei das S/A, na qual há previsão expressa para utilização das "*stock options*", cujo vesting é um dos tipos possíveis, em seu art. artigo 168, § 3º, da Lei 6.404/76.

Todavia, prevalecem na economia brasileira as sociedades limitadas, sendo vedada de integralização de quotas por meio de prestação de serviços, conforme previsão do art. 1055, §2º, do Código Civil, o que incompatibiliza o *vesting* com este tipo societário. Assim sendo, a sociedade anônima seria o tipo societário mais adequado e recomendado para aqueles que desejam utilizar o contrato de *vesting* como forma de atrair reter talentos.

Embora haja muitas tentativas por parte dos operadores do direito o sentido de flexibilizar esta norma e adequar o *vesting* às sociedades limitadas, há que se tomar os devidos cuidados também quanto a aspectos trabalhistas e tributários, os quais não cabe aqui aprofundar, mas que podem comprometer os negócios levando-o ao fracasso antes dele decolar. O uso indiscriminado do *vesting* com a finalidade de burlar a legislação trabalhista certamente poderá trazer mais problemas do que soluções no médio prazo, uma vez que o direito do trabalho é regido pelo princípio da primazia da realidade.

Embora ainda esparsa, a jurisprudência da Justiça do Trabalho[98] têm indicado que, as "*stock options*", por serem financeiramente suportadas pelo próprio empregado, mesmo que com preço diferenciado fornecido pelo empregador, não têm a característica da figura salarial prevista na CLT e na Constituição. Logo, por não representarem garantia de lucro, mas mera expectativa de direito sujeita a oscilações de mercado, possuem natureza jurídica mercantil e não trabalhista. Todavia, em sentido contrário, o Conselho Administrativo de Recursos Fiscais têm entendido e sinalizado que as "*stock options*" convencionais têm caráter remuneratório por não trazerem risco real ao beneficiário, não terem onerosidade em sua aquisição e serem um instrumento outorgado de forma "automática" aos beneficiários[99].

Para evitar eventuais transtornos é fundamental que o plano de opção de compra de ações, instrumento que efetivamente norteia a participação acionária dos empregados, observe sempre os seguintes fatores: i) preço de emissão da ação, ii) prazo para obtenção da elegibilidade do exercício das opções (prazo de carência ou "vesting") e iii) prazo máximo para o exercício das opções (termo da opção).

Vale ressaltar também que os elementos constitutivos da relação de emprego são: i) a alteridade, ii) a subordinação, iii) a

[98] http://www.lassori.com.br/contrato-de-vesting/
[99]https://pris.com.br/blog/decisoes-ineditas-da-camara-superior-do-carf-sobre-planos-de-stock-options/

pessoalidade, iv) a onerosidade, e v) a não eventualidade. No *vesting* os dois primeiros não se configuram, visto que os riscos do negócio passam a ser compartilhados entre empregador e empregado e não há subordinação, uma vez que os cronogramas de atividades são ajustados de forma consensual entre as partes.

Independente da forma ou da natureza jurídica do *vesting* é fundamental que se entenda o problema que deu origem a esta modalidade de contrato, que é: como dividir as ações de uma empresa de forma justa entre acionistas, investidores e funcionários, de forma a recompensar o esforço e o risco assumido por cada um na sociedade, equacionando a expectativa de lucro futuro com a realidade de crescimento do negócio. Não por acaso, poucos temas causam mais falhas nas equipes de *startups* do que as divisões de ações. Neste sentido, Bill Harris afirma que: "As opções de ações não são apenas um caminho para a riqueza, ele diz, mas a ferramenta mais poderosa à sua disposição na construção de um negócio de sucesso. (...) Você precisa de pessoas que estejam dispostas a correr riscos. E então você precisa recompensá-las. (...) Para o funcionário, é ainda melhor. Eles se beneficiam com o aumento do preço das ações e estão protegidos de suas quedas."[100]

[100]https://www.forbes.com/sites/meghancasserly/2013/03/08/understanding-employee-equity-bill-harris-sxsw/#5c3004cb2d72

Um estudo de 2016, T. & N. Wasserman, "*The First Deal: The Division of Founder Equity in New Ventures*"[101], descobriu que 73% das equipes dividiram o patrimônio no primeiro mês da startup, no auge da incerteza sobre a estratégia e o modelo de negócios de suas *startups*, suas funções e seus níveis de comprometimento. A maioria das equipes mal dedicou algum tempo discutindo a divisão, evitando conversas difíceis, porém necessárias para realmente entender as contribuições e intenções de cada um para o negócio. Além disso, a maioria das *startups* dividiu as ações estaticamente - o que significa que as equipes não permitiram ajustes futuros. O resultado desse aperto de mãos precipitado é que a maioria das empresas sofreram uma penalidade significativa pela capacidade reduzida de levantar a primeira rodada e pela valorização abaixo da média. Além do custo financeiro, as tensões internas destrutivas causadas por uma divisão de ações ruim são muitas vezes ainda mais devastadoras.

Dito isso, cabe então analisar as origens do *vesting* para que se possa entender as raízes desse problema para pensar em alternativas e soluções inovadoras para o futuro. Apesar de solucionar parte do problema, já se sabe que muitos outros problemas surgem do modelo de vesting tradicional adotado pela maioria das *startups,* baseado em critério de tempo. Nos

[101] https://lloydmousilli.com/2017/06/20/how-to-slice-the-startup-equity-pie-a-guide-to-slicing-pie/

próximos capítulos serão analisados as diferentes variantes de "*stock options*", que têm surgido ao longo do tempo e o *vesting* pode ser aprimorado.

1. As origens do vesting

Embora seja muito difícil apontar com precisão a origem do contrato de *vesting*, pode-se afirmar que as empresas Fairchild e Hewlett-Packard[102] foram precursoras dessa prática há cerca de cinquenta anos atrás. A abordagem de gerenciamento da Fairchild enfatizava a meritocracia e a abertura sobre a hierarquia, inspirada na abordagem da Hewlett-Packard de "*management by walking around*". Isso incentivou a interação direta dos funcionários, que evoluiu para o estilo distinto de gerenciamento atual do Vale do Silício, baseado em estruturas corporativas "planas" e com ênfase nas habilidades técnicas em relação a outros fatores.

Vesting é uma modalidade de contrato derivada das opções de compra. Apesar de muito comuns no mercado financeiro, as opções de compra têm suas raízes em centenas de anos - muito antes de começarem a ser negociados oficialmente em 1973. Embora as opções tenham sido negociadas ao longo

[102]CASTILLA, E. J. HWANG, H. GRANOVETTER, E. GRANOVETTER, M. TheSilicon Valley Edge: a habitat for innovation and entrepreneurship. Editada porChong-Meon Lee, Willian F. Miller, Marguerit Gong Moncook e Henry S.Rowen.. Stanford University Press. California, 2000.

da história dos EUA, a negociação de opções de ações nos volumes atuais e pelo investidor individual é um fenômeno relativamente recente. A maior parte do comércio de opções antes de 1973 havia sido realizada por agricultores e empresas que buscavam proteger sua exposição agrícola.

Um contrato de opção de compra de ações dá ao detentor o direito de comprar ou vender um número definido de ações por um preço predeterminado, dentro de um prazo definido. Os primeiros registros das opções de compra de ações estão relacionados aos "*Bucket Shops*", que eram corretoras envolvidas em práticas comerciais antiéticas. Historicamente, o termo era usado para se referir a empresas que permitiam que seus clientes apostassem nos preços das ações, geralmente usando níveis perigosamente altos de alavancagem. Mais recentemente, o termo passou a ser associado a empresas que praticam *bucketing*, ou seja, que lucram com as negociações de um cliente sem o seu conhecimento.

As "*Bucket Shops*" tornaram-se bastante comuns no final de 1800, quando a disseminação de novas tecnologias de comunicação, como o telégrafo, tornou possível especular sobre os preços das ações em tempo hábil. Esse tipo de corretora permitia que seus clientes apostassem nos preços das ações da mesma maneira que poderiam apostar em cavalos de corrida. Uma das explicações para a origem do nome "*bucket shop*" se deve à prática de jogarem os bilhetes comerciais em um balde e

depois de misturá-los a empresa sorteavam os vencedores para clientes específicos que pudessem gerar mais lucros. As "*Bucket Shops*" se tornaram muito populares nos Estados Unidos na década de 20, graças a Jesse Livermore. Este empresário atuava como um apostador especulando sobre os movimentos dos preços das ações.

Mas, quando foi que a primeira negociação de opções ocorreu? As primeiras opções foram usadas na Grécia antiga para especular sobre a colheita da azeitona; no entanto, contratos de opção modernos geralmente se referem a ações. A maioria dos historiadores consideram a "Bolha das Tulipas" de 1637 como sendo a primeira vez em que as opções foram usadas. Durante a década de 1630, os bulbos de tulipas na Holanda começaram a se supervalorizar. Algo semelhante à bolha das "pontocom" no final dos anos 90. Diante da escalada de preços dos bulbos de tulipas as opções de compra tornaram-se derivativos populares durante esse período por duas razões: atraso na entrega e alavancagem.

Os comerciantes de tulipas começaram a vender flores que não estariam prontas para entrega. Isso criou o mercado perfeito para futuros e opções de compra, pois os compradores, especulavam que o preço das flores no futuro seria maior do que quando plantadas. Assim começaram a firmar contratos de compra e venda de flores a um preço especificado e em uma data futura. Por esse direito, eles pagariam ao vendedor de flores um

valor independentemente do preço das flores no futuro. Em meio à especulação, quando o primeiro comprador deixou de honrar o seu contrato, isto fez com que os preços das tulipas caíssem para um centésimo de seus valores anteriores, dando origem depressão econômica que durou vários anos e gerou uma considerável desconfiança a investimentos especulativos por parte dos holandeses[103].

Com o passar dos anos as "*stock options*" foram se diversificando, ficando mais complexas e ganhando regulamentações específicas, sendo o *vesting* uma das espécies desse gênero principal. Basicamente as opções podem ser divididas em dois tipos: "*calls*" and "*puts*". As "*calls*" dão ao comprador da opção o direito, mas não a obrigação, de comprar o estoque subjacente a um preço predefinido, conhecido como preço de exercício. Já as "*puts*" dão ao comprador da opção o direito, mas não a obrigação, de vender o estoque subjacente a um preço especificado. Cabe então analisar caso a caso os tipos de *vesting* e as novas tendências que estão surgindo em matéria de "*employee stock options".*

2. Vesting com base em tempo

[103] VERSIGNASSI, Alexandre. Crash: uma breve história da economia – da Grécia Antiga ao séc. XXI. São Paulo: Leya. 2011.

Historicamente, os cronogramas de aquisição de ações em *stock options* geralmente se baseiam no tempo.[104] Embora não haja nenhuma norma específica determinando o *vesting* com base no tempo, provavelmente esta se tornou a fórmula de aquisição mais comum para novos funcionários, sendo estabelecido via de regra um período de aquisição de quatro anos com um quarto do investimento após um ano e os três quartos restantes com aquisições mensais, durante os trinta e seis meses restantes do período de quatro anos.

Vesting é um conceito popular entre *startups*. O seu principal objetivo é reter os fundadores e profissionais talentosos, incentivando-os a permanecer na empresa por um determinado período de tempo. É uma maneira de tentar distribuir as ações de forma equânime. No *vesting* as ações de uma empresa são emitidas, mas a propriedade somente se torna permanente quando determinadas condições forem atendidas. Essa condição geralmente é a mesma: que um profissional permaneça na empresa por um certo número de anos e faça seu trabalho corretamente.

As origens do *vesting* baseado em tempo são uma verdadeira incógnita. Porém existem algumas razões pelas quais a sabedoria convencional favorece o critério baseado no tempo. Trata-se de um conceito simples, fácil de implementar e que

[104] https://www.lexology.com/library/detail.aspx?g=6372b426-6906-4bfa-ba93-9956dfcfbf7e

deixa pouca margem para discussão. Entretanto, por mais certa que possa parecer a medição do tempo, ainda assim, é difícil que sua simples passagem possa se correlacionar de maneira previsível e consistente com a geração de valor de um negócio.

Existem inúmeras variáveis internas e externas que podem influenciar a criação de valor de uma *startup*, isso é algo totalmente imprevisível. Para lidar com esse tipo de incerteza típica de negócios inovadores, a fim de garantir um alinhamento mais coeso e confiável entre sócios, investidores e funcionários com os objetivos chave da empresa, começaram a surgir outros tipos de *vesting*, como o baseado em marcos e resultados.

3. Vesting baseado em marcos e resultados

Embora, a princípio, possa parecer muito eficiente, o *vesting* baseado em marcos e resultados também carrega consigo certa dose de incerteza e imprecisão, que podem gerar conflitos ao longo da relação jurídica estabelecida entre acionistas, sócios fundadores e funcionários vestados.

A regra geral desse tipo de *vesting* é incentivar e motivar os membros da equipe a realizar seu trabalho e gerar valor para o negócio. Infelizmente, embora na teoria isso possa parecer uma excelente fórmula, na prática pode ser bastante problemática. Um dos maiores problemas vêm do fato de marcos e resultados, ao contrário de unidades de tempo, não são fixos

tampouco objetivos, principalmente em se tratando de *startups*, onde as coisas mudam rapidamente a todo instante.

Essa dinâmica inconstante do ambiente de *startups* coloca um grande desafio para a definição de marcos e resultados, uma vez que os resultados esperados para os 4 anos seguintes, no momento da assinatura do contrato de *vesting*, podem simplesmente mudar no próximo mês ou na próxima semana. Isso pode gerar inúmeros conflitos de interesses na empresa.

Talvez, por esta razão, como diz Michael Best: "Atingir marcos de negócios certamente parece uma medida melhor de "valor agregado" do que a simples passagem do tempo e, afinal, toda a ideia de investir é recompensar as pessoas por agregar valor, não por passar o tempo. E, no entanto, o *vesting* baseado em tempo ainda é a regra no mundo das *startups*."

Os planos de negócios das *startups* costuma ser bastante fluidos. Algumas delas sequer os utilizam na prática, optando apenas pelo *Canvas Business Model*. Outro problema, é que alguns marcos e resultados podem ser alcançados muito antes do esperado ou previsto pelos sócios fundadores, tornando o "funcionário vestado" ocioso neste caso.

O ponto principal da aquisição baseada em marcos e resultados é que a teoria parece convincente, mas a realidade é bastante confusa e aleatória. Quanto mais específico o marco, menor a probabilidade de sobreviver intacto durante o período

de *vesting*. Quanto mais genérico for o marco, maiores as chances de haver discordâncias internas e atritos sobre o que significa de fato alcançá-lo ou não. Nada impede, entretanto, a utilização de modelos híbridos de contrato de *vesting*, baseados em critérios de tempo e de resultados.

4. Slicing pie

Visando encontrar um ponto de equilíbrio para os problemas do *vesting* baseado em tempo ou em marcos e resultados, Mike Moyer[105] desenvolveu o método "*slicing pie*". Neste modelo proposto por ele, existem dois tipos de contribuições a serem consideradas nos cálculos: contribuições monetárias em dinheiro e as não monetárias, tais como tempo, propriedade intelectual, instalações, suprimentos, equipamentos e até relacionamentos importantes com potenciais clientes ou investidores. Cada fatia do negócio ("*slice*") representa uma contribuição de risco normalizada. Uma fatia é uma unidade fictícia usada para representar o valor justo de mercado ajustado de uma contribuição em risco, ela não representa ações patrimoniais, nem possui valor real.

A vantagem desse modelo é que ele torna a distribuição de ações dinâmica, variando de acordo com o tempo, mantendo

[105]https://review.chicagobooth.edu/entrepreneurship/2017/article/how-split-equity-without-drawing-blood

as expectativas de cada membro do time alinhadas com a realidade das entregas de valor realizadas por cada um. A qualquer momento, a fórmula acima do "*Slicing Pie*" poderá fornecer um *equity* razoável, ajudando também a calcular o preço justo de compra das ações, caso alguém decida deixar a sociedade antes do *breakeven*.

Com este método, Mike Moyer buscou minimizar os riscos de tentar prever o futuro de uma *startup*, criando um modelo dinâmico para a distribuição de ações ao longo do tempo, que auxilia a reduzir os atritos de interesses internos em uma equipe. Existem dois componentes principais desse modelo dinâmico: uma estrutura de alocação (que diz quanto cada pessoa deve receber) e uma estrutura de recuperação (que diz o que fazer quando alguém sai da empresa)[106].

5. Wealthfront equity plan

Outro modelo que tenta criar uma forma mais justa de alinhar os riscos aos interesses futuros em uma *startup* é o Wealthfront Equity Plan[107], que foi desenvolvido para lidar especificamente com os quatro casos mais importantes de concessão de patrimônio aos funcionários: i) novas

[106] MOYER, Mike. Slicing Pie: Fund Your Company Without Funds. Lake Shark Ventures, LLC, 2012.
[107] https://firstround.com/review/The-Right-Way-to-Grant-Equity-to-Your-Employees/

contratações; ii) promoções; iii) gratificação por desempenho; iv) subsídios perenes.

Ao invés de um processo *ad-hoc*, o Wealthfront Equity Plan oferece um programa transparente, consistente e justo de subsídios patrimoniais que os funcionários podem criar dentro de suas expectativas de longo prazo. Como resultado, é possível vincular a posse e a contribuição de longo prazo à sua participação acionária. Dessa forma, à medida que a empresa cresce, vão sendo concedidos novos *pools* de opções de compra de ações proporcionalmente ao que é justo hoje, e não proporcionalmente à concessão original.

A principal desvantagem deste modelo de planos de opção de compra de ações para a empresa é a possível diluição do patrimônio de outros acionistas quando os funcionários exercem as opções de compra de ações.

6. Reverse vesting

Existe também um tipo de contrato muito utilizado no mercado *venture capital* que é o "*reverse vesting*". Neste tipo de contrato, os fundadores são vestados, não detendo o controle total das suas ações caso deixem a empresa antes do período de aquisição. Nesta hipótese, a empresa tem o direito de recompra ou confisco das ações ainda não vestidas pelo sócio retirante, por uma taxa nominal ou em alguns casos sem custo nenhum.

Os acordos de aquisição de direitos com cláusula de "*reverse vesting*" podem ser celebrados em um acordo de acionistas entre os fundadores na incorporação ou em um estágio posterior quando um investidor entra na sociedade. Trata-se de um mecanismo cujo objetivo principal é manter investidores protegidos, na medida em que querem ter certeza de que os fundadores não abandonem repentinamente o negócio logo após o aporte de capital de risco.

Se por um lado o "*reverse vesting*" garante uma maior proteção para os investidores podendo atraí-los para o negócio, por outro esta cláusula podem representar menos controle e maior risco para os sócios fundadores. Porém, como contrapartida durante o período de aquisição, os cofundadores mantêm todos os seus direitos vinculados às suas ações, incluindo o direito de voto nas assembleias gerais ou o direito a dividendos.

Os acordos de aquisição reversa são mais frequentemente assinados como parte do primeiro grande investimento em uma startup. No entanto, os fundadores às vezes os antecipam e os incluem nos acordos de seus fundadores. Cada fundador recebe garantia de que seus cofundadores estão comprometidos com sua empresa.

7. Vesting coletivo com cláusulas de preferência

Em tese haveria a possibilidade também de se adotar o *vesting* coletivo com cláusula de preferência, porém até a data deste artigo não foi possível encontrar nenhuma literatura a respeito desse modelo de contrato. Na prática este tipo dinâmico de *vesting,* permitiria alinhar os interesses de expectativas de um grupo de funcionários vestados, garantindo àqueles que entregarem maior valor ao negócio o direito preferencial de aquisição das contas remanescentes dos demais, podendo, dessa forma, obter um número até maior de ações do que as negociadas inicialmente.

O efeito psicológico do vesting coletivo com cláusula de preferência seria similar a um processo de gamificação, movendo os funcionários vestados em busca das ações remanescentes, aumentando assim suas expectativas futuras em relação à sua participação na sociedade e criando um *flow* de engajamento onde os ganhos podem ser maiores do que os esperados de acordo com o mérito de cada um.

Concebido para assegurar a manutenção do equilíbrio societário, evitando que abusos causem a diluição da participação do acionista no capital social, o direito de preferência para a subscrição de ações está previsto na Lei de S/A como um dos direitos essenciais do acionista (art. 109, IV). O intuito da lei, neste caso, é evitar que acionistas antigos e minoritários sejam diluídos por meio da emissão de ações,

garantindo-lhes uma salvaguarda para manter a mesma posição que detinham antes do aumento do capital.

Trata-se, portanto, de um instituto que visa defender o acionista contra os riscos da diluição da sua participação no capital social, a qual pode ter consequências sobre os direitos dos acionistas. A lei atual permite que o direito de preferência seja exercido não só nos casos de integralização em dinheiro, mas também por meio de capitalização de créditos ou subscrição em bens (art. 171, § 2º).

Note-se que o modelo proposto visa estabelecer uma espécie de motivação extra aos funcionários ou sócios vestados, baseada na competição pelas ações remanescentes daqueles que não cumpriram suas metas e objetivos ou que desistiram antes do tempo previsto para o exercício da opção de compra. Embora encontre respaldo no ordenamento jurídico brasileiro, este tipo de contrato ainda não foi testado, não sendo possível sua eficácia em termos de resultados práticos, tornando arriscado do ponto de vista econômico.

Considerações finais

Existem inúmeras modalidades de *vesting* e todas elas apresentam prós e contras, riscos e garantias, vantagens e desvantagens. Não se trata de utilizar este instrumento como uma forma de contratar bons empregados sem pagar o valor

justo pelo seu salário, tão pouco se resume a um cassino de apostas. Cabe a cada empresário entender qual tipo de *vesting* funciona melhor para o seu negócio no sentido de alinhar os interesses dos fundadores, funcionários e investidores, com os objetivos chave da empresa.

Pode-se perceber também que este tipo de contrato está em constante evolução sofrendo mutações inerentes ao ambiente dinâmico e inovador das *startups.* Por isso é fundamental pensar no problema que se quer solucionar e não apenas nas supostas vantagens que se quer obter. Uma vez que, algumas vantagens capciosas podem em muitos casos se tornar prejuízos irreparáveis ao negócio, devendo sempre prevalecer a boa-fé e a lealdade nos negócios jurídicos.

Não se pretendia neste artigo esgotar o rol de tipos de contrato de *vesting*, mas sim ilustrar alguns exemplos clássicos e outros mais inovadores. Ao conhecer as origens do contrato de *vesting* e compreender os problemas que motivaram sua criação, bem como seus elementos fundamentais, é possível pensar neste tipo de contrato de forma aberta, sem se apegar a modelos prontos. Em se tratando de um contrato atípico, desde que compatibilizado com o sistema jurídico de normas e princípios, são inúmeras as possibilidades de utilização do *vesting.*

Referências bibliográficas

BLANK, Steven. The startup owner's manual: The step-by-step guide for building a great company. John Wiley & Sons, 2020.

CASTILLA, E. J. HWANG, H. GRANOVETTER, E. GRANOVETTER, M. TheSilicon Valley Edge: a habitat for innovation and entrepreneurship. Editada porChong-Meon Lee, Willian F. Miller, Marguerit Gong Moncook e Henry S.Rowen.. Stanford University Press. California, 2000.

MOYER, Mike. Slicing Pie: Fund Your Company Without Funds. Lake Shark Ventures, LLC, 2012.

VERSIGNASSI, Alexandre. Crash: uma breve história da economia – da Grécia Antiga ao séc. XXI. São Paulo: Leya. 2011.