Direito e Tecnologia
Prof. Jorge Morais Carvalho
2019/2020

Aula nº2 **26.09.2019**

Tecnologia para o direito: a emergência de novos paradigmas de pesquisa jurídica

Patrícia André

Saber de que forma a tecnologia pode ajudar o Direito e de que forma o trabalho dos juristas pode ser facilitado pela tecnologia.

Duas perspetivas principais para encarar estas realidades:

- Uma entende o direito como processo e a tecnologia a integrar-se no mesmo e;
- Outro que tem que ver com as implicações da tecnologia para o direito e que requerem intervenção deste último. Sendo que estas entrecruzam-se.

Além destas duas, existem outras duas entre as demais:

- Meta abordagem, por um lado numa perspetiva de estudos sociojurídicos, perspetiva externa sobre a sociedade e o impacto tecnologia;
- Meta abordagem, o campo específico da teoria do direito e da inteligência artificial, uma área específica que dá para imensas aulas. É uma área muito particular e que se desenvolve a nível teorético, sobre o (...).

Pesquisa jurídica

- Dupla aceção; estrutura interna da metodologia jurídica no exercício do direito entre os operadores jurídico, tem que ver com a estrutura como o raciocínio jurídico se desenvolve. Desde a identificação dos elementos relevantes para desenvolver esse raciocínio, a argumentação para interpretar direito e a decisão. Tem que ver com a perspetiva da transmissão e processamento da informação jurídica, o mesmo em relação à pesquisa jurídica enquanto método de investigação metodologia do estudo e do ensino em direito. a pesquisa assume-se como uma coisa substantiva, do ponto de vista da investigação é uma característica metodológica que abre campos sistémicos.

Exercício do direito

- Longo ciclo analógico: a transmissão da informação jurídica é feita através de texto que tem de ter suportes. Este paradigma é marcado por continuidade analógica e delinearidade na pesquisa jurídica. Quando trabalhamos só com isto há que haver lógicas de continuidade e de delinearidade, é fulcral para o bom funcionamento desta atividade. Quando as coisas só funcionam em papel estão dispersas, incompletas, é impossível que tudo seja objeto de impressão, pelo que a difusão e o acesso a essa mesma informação é muito restrito. A forma como a legislação era veiculada, era dispersa, por coletâneas, revistas, coleções oficiais e o diário da república, por exemplo, começa em 1715 como Gazeta de Lisboa e só se transforma em Diário da República online em 2006.

- Trabalhos preparatórios da AR, essenciais como fontes de direito, passaram a existir em suporte digital desde 2007. A jurisprudência foi um dos campos em que se começou mais cedo e em 1998 a DGSI surge como base de dados, embora, inicialmente, muito restrita e com poucos documentos e poucos tribunais. As revistas, por exemplo, havia mais de 150 revistas jurídicas entre 1930 e 2000. A coletânea de jurisprudência ficou disponível online a partir de 2008. Os anos 2000 marcam a mudança de paradigma do acesso à informação em rede.

O computador introduz as tecnologias de informação na era digital, o que muda a distribuição e o consumo de informação. Esta passagem predominantemente analogia para digital, faz mudar as técnicas, mas também a forma como é distribuída e se repercute na sociedade. As alterações não são meramente as ferramentas, introduzem profundas alterações no exercício do direito. este mecanismo de passagem é quem faz isso. A internet foi potenciadora neste aspeto e, depois, com a inteligência artificial são inaugurados aqueles que são (...) Este quadro repercutiu-se no mundo jurídico.

Quando estamos a produzir direito passamos a funcionar nesta dinâmica de (..). agora, passamos a ter uma dinâmica de multiplicação e aumento da informação jurídica. É neste sentido que surgem novos paradigmas que nos permitem fazer um trabalho quantitativo, uma triagem.

Se não tivesse existido uma primeira fase, aquilo que temos hoje não teria acontecido. Inicialmente, estas coisas existiam em formatos digitais, mas mais arcaicos do que os que temos agora (DVD's, por exemplo). Durante os anos 2000 houve uma mudança tremenda neste paradigma, embora já digital, a internet revolucionou toda a forma como se passou a aceder à documentação. Assistimos à informatização dos tribunais (CITIUS).

Saímos do paradigma da base de dados porque a comunicação online passou a ganhar dimensões enormes. Começamos a passar para o paradigma das redes e da inteligência artificial. Passamos a estar focados na produção, tratamento, análise e disponibilização dos dados. Aliás, há quem diga que o big data é possível hoje não pela, mas também, exponencial informação, mas pela existência exponencial da informação sobre a informação. Não tivesse sido a base de dados, da coleta e recolha da informação, não era possível hoje termos aquilo que é o big data que nos permite tratar e analisar de forma inteligente e automatizada da informação.

Novo paradigma

- Inteligência artificial: habilidade dos computadores (...) o objetivo é a construção de sistemas computacionais inteligentes, portanto a sua área é interdisciplinar.
- Computação cognitiva: reforço da comunicação entre humanos e os sistemas.
- Outra expressão: mais dramática e catastrófica, defendida por aqueles que consideram que a máquina vai substituir o Homem.

→ Incorpora várias tecnologias que antes eram só do homem, mas incorpora a inteligência humana também.

Machine learning: aprendizagem automática, previsão de comportamentos a partir de exemplos.

Deep Learning: desenvolvimento do *machine learning*. Recupera algo mais antigo que era as redes neurais artificiais. Identificação de padrões, está na base do reconhecimento facial, por exemplo.

Reforcement learning: estímulo para a ação com base nos mecanismos computacionais. A aprendizagem automática torna-se num reforço, está na base dos veículos autónomos.

Subáreas e os objetivos que se pretendem dentro da tecnologia

→ Por um lado, a recuperação da informação a partir de material não estruturado, normalmente texto; a extração da informação (mineração de texto).

Estado de arte global

- *Legal expert system*: é a tecnologia que está na base da criação da figura do advogado virtual. A arquitetura da linguagem, da parte técnica caiu ao fim de alguns anos e aquilo que sobrou tem que ver com a lógica dos serviços jurídicos online enquanto assistente jurídico do ponto de vista do cidadão.
- *E-discovery*: a inteligência virtual ganhou outra ação. Tem que ver com o processo de descoberta da informação relevante. O processo de descoberta passa por reunir, descobrir e identificar a informação. São ferramentas que permitem fazer essa descoberta e identificação e que identificam se são ou não relevantes para a questão que temos em mãos.
- *Legal research*: em termos estritos de pesquisa jurídica
- *Legal analytics*: a grande área hoje em dia, precisamente porque aproveita as ferramentas que vêm do *machine, deep e reforcement learning* e que servem para analisar (...)

→ Em Portugal não há dados públicos, mas por exemplo a PLMJ tem um sócio especializado em software e inteligência artificial: *Kira* ferramenta de software em Portugal.

Aula nº3 **03.10.2019**

Aspetos técnicos da tecnologia *Blockchain*

Matheus Passos Silva

Definições técnicas iniciais

- *Blockchain* não é algo novo (desde 1991, Stuart Sber e W. Scott Stornetta) que existe um artigo sobre os conceitos de uma *Blockchain* embora não usassem este termo em nada, falavam de tudo aquilo que está presente neste conceito. Esta tecnologia é um conjunto de conceitos da área da informática (criptografia, registo distribuído, mineração). Estas tecnologias não são de 2009, 2000, são da década de 40/50 do século passado. Juntou-se tudo e criou-se aquilo que temos hoje.
- A sua estrutura consiste essencialmente num conjunto de dados armazenados em grupos chamados blocos. Cada bloco validade é vinculador ao bloco anterior por criptografia. Podem ser guardados quaisquer dados, embora existam recomendações sobre o que deve ou não deve ser colocado nesses blocos.
- Um bloco x, tem dados gravados por alguém; bloco y, dados gravados por alguém, bloco z e assim sucessivamente. Esses dados são gravados de forma sequencial. Cada bloco depende necessariamente do outro, anterior.

Características

- Criptografia: cada bloco vai ser gravado na sequência e digamos que o bloco posterior só vai ser gravado em decorrência de determinados cálculos criptográficos que são dependes do bloco anterior.
    - *Hash*: é uma espécie de impressão digital do bloco. Uma vez que se cria o *hash* de um determinado conteúdo, aquele *hash*, há menor alteração que se faça no

conteúdo, altera-o de forma completamente aleatória. É um número em formato hexadecimal. Corresponde a um número de identificação de 64 dígitos.

- Hash SHA-256.

Uma vez criado o *hash* ele é fácil de calcular; difícil é determinar o contrário, ou seja, se coloco a frase "titulo da apresentação" e uma calculadora de *hash*, ele dá como resultado um número *hash* com 64 digitos hexa decimal. Apesar do conteúdo para nós humanos ser o mesmo; quando se aplica à função *hash*, o resultado é completamente diferente. Não conseguimos fazer uma associação entre os números e os caracteres que aparecem. Quando se cria esta função é praticamente impossível descodificar a função *hash*.

Além da criptografia há outras características técnicas relevantes:

- Registo distribuído: dizer que os dados não estão armazenados num único computador. Bem ou mal, quando uma determinada empresa sofre um ataque, não apenas há violação dos dados, mas aquele sistema pode ficar inacessível porque aquele servidor onde estão os dados foi comprometido. Os dados estão distribuídos em todos os computadores que usam aquela rede (bitcoin: qualquer pessoa que faça download do programa, a partir do momento em que está a ser executado, a pessoa está inserida na *blockchain* do bitcoin, passando a ter gravados todos os dados. Em princípio não há problema, como os dados são criptografados ninguém altera; quem quer tem acesso ao conteúdo, porque em princípio a rede é transparente, mas não se sabe o que vai acontecer porque a rede não tem o nome de ninguém, somente o endereço de quem envia e recebe e os valores transacionados.
- Imutabilidade dos dados: não é possível alterar, os dados são imutáveis; à exceção de um ataque de 51%;
- Transparência: todos aqueles que têm acesso à base de dados sabem o que é que acontece.
- *Append-only:* não se apagam dados de uma *blockchain*, uma vez gravados no bloco x, y e assim sucessivamente. Aquilo que fica gravado no bloco x não pode ser apagado, a menos que ocorra um ataque. Ou seja, os dados gravados não podem ser excluídos.

As características impedem a alteração dos dados, o que é relevante em algumas situações. Mantendo-se a integridade e a sua confiabilidade ao longo do tempo (*proof of existence)*. Por exemplo, o Estado pode criar um registo em *blockchain* para saber se os contribuintes estão a pagar todos os seus impostos.

Não precisa de confiar nas pessoas. Quando hoje as pessoas fazem transferência de dinheiro de uma para a outra, a primeira confiança é dada ao banco. No caso do *blockchain*, a confiança é depositada nas características técnicas, nas transações realizadas pelos envolvidos mesmo que este senão se conheçam, ou mesmo que estes desconfiem uns dos outros.

Bloco 0 ou bloco genesis > dados: data e hora da criação do bloco entre outros aspetos. O sistema faz um *hash*, com 64 caracteres e refere-se ao número do bloco, ou seja, à posição, vai referir-se aos dados e ao seu conteúdo e à data e hora em que os dados foram gravados. Depois, vem outra pessoa que partilha a mesma *blockchain* e quer gravar um dado dela; a partir daqui os dados são gravados de forma sequencial. O bloco 1 tem o *hash* do bloco 0 e vai ser aplicado ao conjunto dos dados do bloco anterior. Ou seja, em todos os blocos vou ter quatro elementos, o *hash* do bloco anterior entre outros dados.

Alguém quer fazer um ataque de 51%: vários blocos gravados em vários computadores, um novo bloco só é adicionado se os outros computadores aceitarem. O ataque é aquela situação

em que a maioria dos computadores de uma rede é utilizada para alterar os dados. Não basta controlar um computador. Para alterar os dados preciso de controlar 500 mil e um computadores ao mesmo tempo e fazer com que esses computadores façam a mesma ação no mesmo milissegundo, ou seja, alterar o *hash*. Quanto maior o número de computadores, mais difícil é o ataque.

Smart contracts

De *smart* não tem absolutamente nada, são apenas códigos. Se ocorrer x, faça y; se não ocorrer x, não faça y, faça z. é nada mais do que um código programado para ser iniciado automaticamente conforme se verifique a existência de determinadas condições pré-estabelecidas.

Os *smart contarcts* rodam na própria rede *blockchain*, de maneira que não apenas o código é distribuído entre todos os participantes, mas também o resultado da execução do *smart contract.*

Ex: seguros do carro: a seguradora instala um ship no carro para saber como foi o acidente; o seguro é acionado automaticamente. A seguradora não faz nada, o segurado não faz nada porque não precisa de papelada e o negócio ocorre de forma automática. Na Ásia existem seguros de plantações: se o tempo tiver muito seco ou chover de mais, a pessoa recebe um seguro. Define-se um critério baseado no nível de chuva; o segurado recebe o seguro automático. É um programa que funciona dentro de uma *blockchain*. Se alguém alterar o código, todos os que estão na rede sabem. Os resultados do programa são gravados nos blocos, portanto não têm como negar.

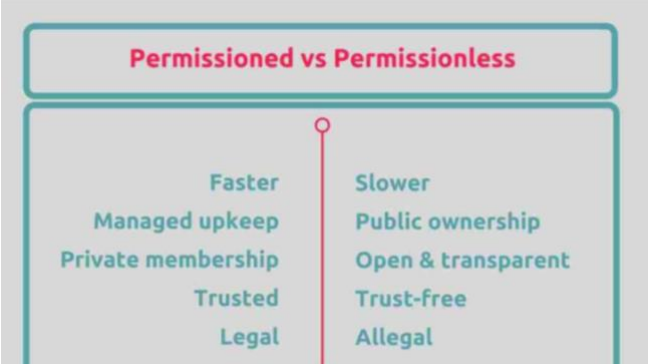
Blockchain público (*permissionless*)

Ex: bitcoin

- Qualquer pessoa pode ter acesso à rede. Ler, gravar e validar (= sim, o *hash* desse conteúdo é verdadeira) dados no banco de dados
- São descentralizadas e nenhuma entidade tem controlo.
- Os dados são gravados de maneira segura, já que não podem ser alterados depois de validados pelos mineradores.
- Se fizer uma transferência internacional, se perder a minha chave privada, que grosso modo é a senha, a quem vou recorrer? Não há ninguém, não há um intermediário.
- O facto de não haver uma entidade não tem de significar necessariamente que a rede não seja segura porque, na verdade, é.

Blockchain privada (*permissioned)*

- Só tem acesso quem tem permissão, através de uma autorização prévia.
- Possuem restrições em relação a quem pode participar e a quais tarnsaçoes podem ser realizadas pelos participantes.
- São redes de empresas em que a empresa não abre para qualquer um, logicamente. Por exemplo, há casos em que existem várias empresas a usarem a mesma *blockchain*. Ex: transporte de produtos da Ásia para a Europa (empresa de telemóveis, transportador, vendedor).



Usos práticos de uma *blockchain*

- Programas de fidelidade,
- Controle de partes de produto,
- Gestão de cadeias de abastecimento,
- Registo de ativos, identidade dos cidadãos,
- Identidade dos cidadãos,
- Votações,
- Soluções de disputas;
- Controle de registos médicos.

Casos práticos na UE

- Suíça: verificação de identidade, votações e aluguer de bicicletas;
- Finlândia: registo de refugiados e controle de benefícios distribuídos por cartão de debito;
- Suécia: transferência de títulos de propriedades e registos médicos;
- Reino Unido: registo e propriedades:
- Malta: certificados

→ *Blockchain* é a tecnologia que permite a existência de criptomoedas.

Blockchain no combate à corrupção: ferramenta da OCDE

- Divisão anticorrupção: programa estabelecido em 1998 em que participam 25 países da Ásia central e Europa ocidental.
- Objetivo: troca de informações.
- Problemas antes da *blockchain*: as bases de dados estavam frequentemente desatualizadas.
- As informações eram enviadas apenas aos contactos centrais do país – cabia a estes divulgar às demais autoridades, o que nem sempre era feito.
- Ausência de controle do OCDE na divulgação das informações.
- Ausência de resposta (resposta demorada) a respeito das ações desenvolvias no país com base nas orientações da OCDE.

Soluções

- A partir de 2018 surgiu a ACN Blockchain Platform: plataforma online que melhora a cooperação internacional entre os países da rede e está em pleno funcionamento.
- Criação de um banco de dados de contactos;
- Criação de um serviço de mensagens seguras para troca de informações informais entre os envolvidos.
- Estabelecimento de nova base de dados sobre os casos de corrupção ocorrendo nos países participantes;
- Criação de uma nova base de dados com legislação a respeito do combate à corrupção.
- Objetivo geral do projeto: confirmar o momento de atualização e de troca de mensagens (*timestamping*).
- Forma de pressionar os envolvidos a agirem confirme as situações com as quais se deparam.

- Possibilidade de auditoria em tempo real do que estiver ocorrendo – transferência de valores, de informações e/ou documentos.
- Efeito secundário: combate às *fake news*; aos dados falsos, à contrafação, à alteração proposital de dados.

Estudo do caso da Estónia:

⇒ Maior exemplo de uso de *blockchain* para o mais variado tipo de registo de âmbito público.

Desde 1997 oferece serviços públicos em formato online: declaração do IRS demora 5 min a ser feita; investe no *blockchain* antes do aparecimento do *blockchain* associado à bitcoin. Todo o seu sistema de saúde é registado em *blockchain*. Receitas médicas são só fornecidas por meios digitais, por meio de *blockchain* e as farmácias estão integradas (médico- paciente/utente-farmácia).

À exceção do casamento, divórcio e transações imobiliárias, todas as demais operações relacionadas com o Estado podem ser feitas através do meio digital.

- Desde 2008 investe em *blockchain*;
- Desde 2012 todo o registo de propriedade é feito em *blockchain*;
- A *blockchain* é usada para garantir a integridade dos dados (uso da função *hash)*;
- O *hash* é gravado no *blockchain*, que devolve a data e hora do registo (t*imestamping* ou *proof of reigistration*)
- Objetivo geral: garantir a veracidade dos documentos.
- O sistema da Estónia permite que qualquer cidadão verifique, a qualquer momento, quem visualizou as suas informações pessoas.
- Todo o sistema de saúde da Estónia também é registado em *blockchain*.
- Outros registos em *blockchain*: Diário Oficial d Estónia, registo de veículos, abertura de novas empresas, sistema digital dos tribunais, sistema de vigilância.

Breve reflexão: Steve Ballimer, 2007

→ Prefere estudar isto agora, mesmo que daqui a 10 anos já não exista do que não estudar de todo e depois arrepender-se.

Aula nº4 **10.10.2019**

Criptomoedas e outras aplicações jurídicas de *Blockchain*

Martinho Lucas Pires

Para que serve e problemas das suas aplicações:

A *blockchain* é no fundo uma base de dados digital, um software que qualquer um pode descarregar e que serve para partilha, armazenamento, registo de dados numa forma comum, descentralizada e que permite transparência, segurança e eficiência do próprio registo. Funciona, numa primeira camada sobre a internet, ou seja, é uma aplicação online. Numa segunda camada, a *blockchain strictu sensu* é a rede: é o local onde vai estar o registo, os blocos com a informação. Numa terceira camada, temos as aplicações.

Os protocolos de *blockchain* não são todos iguais, aliás, nem têm esta terceira camada (Ex: *bitcoin*). Esta terceira camada serve para programas informático. Na rede, faz-se o registo dos dados onde a *blockchain* cumpre a sua função. As aplicações funcionam quer ao nível da rede quer ao nível das aplicações.

A mais conhecida é a dos criptoativos. As criptomoedas são um meio de pagamento para realizar trocas comercias, completamente virtual. É uma informação, um dado binário que está numa rede, emitida por uma rede através de um algoritmo pré-programado da rede. Os *miners* são utilizadores que votam o seu poder informático para tentar resolver um problema informático preestabelecido na rede, resolvem um problema e criam um novo bloco. Com isso recebem bitcoins. A bitcoin não é moeda no sentido jurídico nem tem curso legal. Por exemplo, um comerciante não está obrigado a aceitar um pagamento em bitcoin. A bitcoin foi criada apenas para ser um meio de pagamento, sem estar dependente de Estados ou de instituições bancárias. Têm o valor que lhe quisermos atribuir. A grande inovação da bitcoin é ser completamente digital, não tem existência física e é imutável. Há um número limite de bitcoins no mundo (250 milhões, máximo). São ativos digitais, únicos, podem ser circulados facilmente entre várias pessoas. Do ponto de vista jurídico, variam consoante o seu propósito e utilização.

Outros criptoativos não são utilizados para serem apenas moeda, por exemplo: *ether* (ETH)-*Etheriam:* criação de aplicações digitais através de uma *blockchain*, têm informações sobre as aplicações, em que é que estão a ser utilizadas e quaisquer outros dados. O *ether* é um meio de pagamento interno na rede. Através do *ether* conseguiam comprar mais espaço na *etherian* e depois criar aplicações cada vez maiores; *ripple* (XRP): é um ativo digital que serve para facilitar trocas interbancárias. Para fazer uma transação internacional tem de haver uma certificação da mesma. No fundo, a *ripple* quer acaba por o token, através do XRP. A KIK (whatsapp da Ásia) quis criar um *token* para angariar capital e fazer uma série de projetos. O *token* emitido pelo kik não era uma ação nem uma criptomoeda mas sim um conjunto de direitos que o detentor do *token* teria. Depois temos tokens que não têm nenhuma espécie de direitos dos seus utilizadores, mas que podem ser geradores de valor por si só porque podem ser trocados em plataformas para o efeito, no fundo são redes externas a esta rede, são os *gatekeepers*; permitem comprar criptomoedas e valorizá-las (bolas de valores). Consoante o seu potencial especulativo, começava a ter valor e era circulado. Há *tokens* que são puramente especulativos, não têm valor acrescentado e não representam qualquer direito.

- *Currency tokens*: bitcoin – meio de pagamento, não representa nenhum direito sobre nenhuma outra realidade;

- *Security tokens*: representam direitos sobre o capital da sociedade, por exemplo, ou que são especulativos;

- *Utility tokens*: cartões cliente, dão direitos dentro da rede para um conjunto de serviços que a rede proporciona.

Na prática, esta distinção é mais complexa porque há *tokens* com mais do que uma característica.

As redes servem para além de ter tokens. Por exemplo, há redes privadas que não dependem de validação. Por exemplo, muitas utilizações em redes públicas (Geórgia) são feitas para fazer registos, como o registo de propriedade.

No transporte marítimo há um problema grave de seguros, porque estão envolvidos muitos. Se há um dano, a seguradora vai tentar provar que não tem responsabilidade naquilo. Se há um acidente entre Bali e Tóquio, é a seguradora do navio que vai ser ativada.

As *stable coins* permitem uma maior segurança e estabilidade na utilização.

Steem: aplicação construída a partir da rede *Etheriam*. São muitas vezes construídas a partir de comandos automáticos. Estes comandos, os *smart contracts*, são elevadas um bocado ao extremo, podendo levar à criação de organizações automáticas.

Problemas jurídicos:

- Aplica-se a regulação sobre os meios de pagamento? À medida que o mercado vai aceitando pagamentos com bitcoins....
- *Security tokens*: não é tão utilizada, ou utilizada apenas em jurisdições com regulação própria (Malta, França, por exemplo)
- Própria qualificação de um criptoativo com qualificação jurídica:

Com ativos digitais, os próprios contratos tornam-se ativos digitais e a autenticação já está feita, não sendo necessárias burocracias. Contudo, o facto de estar online pode ser alvo de furto ou outras ações ilícitas.

Blockchain e RGPD: como conciliar a imutabilidade dos dados e a impossibilidade do apagamento com o direito ao esquecimento do RGPD? Blockchain europeia: poucos utilizadores, a questão ainda está em aberto, projeto em desenvolvimento.

As redes de *blockchain* são descentralizadas, mas o poder computacional que alimenta essa rede está sediado em dois ou três territórios e em alguns autores específicos.

Aula nº5 **16.10.2019**

Inteligência artificial: desafios legais

Mascarenhas

O que é que a IA e qual a sua relação com o Direito

Enquadramento geral e sumário que a utilização da IA coloca ao Direito.

Enquadramento

- A IA é algo muito recente, sendo que o seu surgimento remonta ao final dos anos 60.
- Descodificação do código do enigma: filme jogo da imitação.
- 1955: matemático criou o conceito de IA e, reunindo um conjunto de cientistas de diversas áreas, procurou debater se era possível que todos os aspetos da inteligência humana fossem utilizados por uma máquina.
- 1990: investimento por parte das empresas ligadas ao hardware, com investimento em algoritmos.
- 2005: veículos autónomos, siri, reconhecimento de voz, etc.

O que é que mudou?

As máquinas, a capacidade de processamento, os dados e as redes. Isto tudo ligado com um sistema tecnológico que, em interação, permite uma capacidade de análise, fluxo, e tratamento de dados que não era existente há uns anos atras.

Conceitos

- A IA não deixa de ser um sistema que permite realizar tarefas que estão associadas à inteligência humana de forma autónoma e racional. A academia procura dissociar a IA da inteligência humana, gostando mais do termo agentes inteligentes.

- A UE veio dar uma definição, considerada abrangente: aplica-se a sistema que apresentam comportamento inteligente capazes de adaptarem e aprenderem através de diferentes situações alcançando objetivos complexos.

Uma definição de IA fornecida por um grupo designado pela CE: "Comunição sobre o projeto inteligência artificial na europa 2018". É uma definição descritiva, detalhada com carácter pedagógico, mas que não serve para aferir aquilo que é a IA. De uma forma simples, *mais não é do que um sistema que permite na sua interseção com os dados aprender e aferir dados sem qualquer intervenção humana.*

A aprendizagem automática permite um algoritmo que é alimentado por dados e que mediante a identificação de determinados padrões toma decisões sem qualquer intervenção humana. O programador orienta o algoritmo no sentido de introdução de um determinado padrão, recorrendo a silogismos; depois, o algoritmo face aos dados vai alimentando e aprendendo os resultados, tomando decisões consoante a informação que obtém.

A robótica tem um suporte físico associado e tem uma interação com o meio ambiente onde atuam. O nível de autonomia pode ser maior ou menor.

O próprio nome é criticado porque a questão de o que é inteligência pode ser bastante debatido, mas a associação ao comportamento humano leva a algumas problemáticas do ponto de vista ético e jurídico.

Desafios

Não são muito diferentes dos problemas que colocam qualquer tecnologia. No fundo é saber como é que com a utilização se garante que os nossos valores fundamentais são respeitados, como é que vão funcionar corretamente, como é que é programam, qual é a capacidade de autoaprendizagem do próprio sistema e o impacto que tem na segurança física e virtual e como é que podem ser responsabilizados em caso de danos.

Problemas inerentes ao uso da IA

- A questão dos dados: nem sempre são corretos, a sua qualidade pode não ser suficientemente trabalhada e induzir a resultados pouco corretos.
- São dados estatísticos colocando em causa a sua qualidade;
- Ao contrário de um *software* em que se dão ordens para a programação, sendo que o mesmo executa a tarefa; aqui, nos sistemas de aplicação em IA consegue-se saber o momento de entrada dos dados e depois sabe-se o resultado. Há um processo de aprendizagem do algoritmo que não se consegue identificar – problema do *black box*. Isto leva a questões de discriminação, enviesamento.

Discriminação na IA

- O risco de enviesamento pode surgir por parte do programador.
- O sistema de reconhecimento fácil utilizado pela polícia;
- Enquanto não se garantir a qualidade dos dados a questão da discriminação continua a existir.
- Quem desenvolve os sistemas tem começado a adotar um código de conduta que é tido e observado pelos programadores. Coloca desafios éticos e à própria ciência jurídica.

Regulação

Coloca desafios de regulação. *O atual código jurídico responde? Será preciso uma nova lei? Ou vale aplicar a legislação existente?*

A diferença reside em dois fatores: modelo antropocêntrico que existe em toda a sociedade, na verdade, a questão da responsabilização pressupõe uma relação com um sujeito de direito e a este associado, para efeitos, a questão da culpa. Depois, a norma é neutra tecnologicamente, não atende à mesma.

Aquilo que o sistema da IA coloca é que, de facto, a máquina pode ir para além da capacidade a nível humano, a máquina pode estar integrada no próprio corpo humano (ex: próteses). Os conceitos que temos e com que trabalhamos e utilizando aquilo que é o conceito das próprias tecnologias vai também definir ou delimitar as fronteiras de aplicação do direito. Por exemplo, *o que é que se faz quando a máquina toma uma decisão que vai em sentido contrário daquela que é a vontade da própria pessoa?* Relação entre o homem e a máquina: aspeto diferente daquilo que acontecia no passado aquando da relação entre o homem e a tecnologia.

Como e que agora vamos tratar os danos pro exemplo que estes sistemas podem causar?

Em termos de regulação há sempre preocupação de as normas não constituírem limites à inovação, uma vez que é essencial seu desenvolvimento. Ao mesmo tempo, como é que garantimos a proteção dos DLG. As questões de regulação continuam a ser as mesmas.

Em termos de responsabilidade, quem é responsável pelo dano? O produtor, o programador, o utilizador ou a máquina? Atendendo ao quadro jurídico vigente, quem será o agente responsabilizador?

O PE equacionou a possibilidade de se atribuir uma personalidade eletrónica à máquina o que permitira resolver algumas questões. Foi uma hipótese muito contestada, tendo a CE afastado essa solução. Outra solução apresentada pelo PE: transferir a questão da responsabilidade da culpa para o risco e para gestão de risco, instituindo um seguro obrigatório que responderia pelos danos causados e os produtores contribuíram para um fundo de compensação, onde a responsabilidade seria limitada em caso de danos. Solução esta que foi criticada no sentido em que não pode dizer que a responsabilidade pode ser limitada, que não está de acordo com a solução proposta pelo PE.

Responsabilidade civil

- Danos causados pelos animais;
- Responsabilidade do comissario pelos atos do comité;
- Incumprimento dos deveres de vigilância.

Todas estas soluções pressupõem a culpa. A questão da inteligência está associada à capacidade de aprendizagem ou a consciência? A máquina não tem consciência, pelo que aqui a questão seria mais difícil de tratar.

A solução mais discutida, levantado sempre problemas, *a questão da responsabilidade do produtor?* É uma responsabilidade objetiva, não existe culpa, mas isto aplica-se a coisas corpóreas: não se aplicava ao *software* nem à programação.

No âmbito destas discussões, a CE está a desenvolver um estudo sobre esta problemática: responsabilidade do produto (eventual extensão para o *software* e *hardware*. É muito difícil identificar uma anomalia, defeito num programa informático. Eu dou instruções que depois são convertidas em códigos. Mas é muito difícil determinar que um determinado dano foi causado por um erro do *software*, quer por uma instrução que devia ter incorporado e não incorporou. A CE entendeu que a responsabilidade deve ser do programador. Mas muitas vezes este trabalha

com uma empresa, não trabalhando sozinho, trabalhando até com várias aplicações. O que tornaria isto muito complexo e prejudicial para o próprio consumidor.

Existe a solução que defende que a responsabilidade é do consumidor: Este não sabe nem conhece verdadeiramente como o sistema funciona.

Posto isto, a tendência será adaptar qualquer uma destas soluções ao caso concreto. Resolver-se-ão não tanto de um ponto de vista de ressarcimento, mas muito pela informação nos contratos e nos consumidores, e a via contratual continua a ser muito utilizada para regular esta questão. O que está a acontecer é que esta *soft law* de resolução de litígios tem sido um elemento orientador que faz com que os Estados vão atrás daquilo que vai sendo feito.
Ex: o Facebook tem dois recursos hierárquicos- comités e peritos magnos. Ou seja, estas entidades privadas vão assumindo o papel dos Estados em proteger os direitos fundamentais dos cidadãos, pelo que algo está mal.) *vs* novas tecnologias

Ética desde a conceção

- Assegurar que a conceção e a aplicação de instrumentos e serviços de inteligência artificial sejam compatíveis com os direitos fundamentais.
- Informação/transparência;
- Avaliação de impacto.

Não só as empresas têm adotado códigos de conduta, mas os próprios programadores também têm. A CE adotou princípios que definem como quadro ético, jurídico e apropriado que promova a inovação e a segurança jurídica com foco nas pessoas.

Quadro para uma IA de confiança

- Mecanismos de responsabilidade;
- A compensação pelos danos não deve ser limitada.

Ética na IA: Europa

Os sistemas de IA têm de ser regulados no quadro regulamentar existente, conforme os princípios éticos e a robustez.

<u>Requisitos chave</u>:

- Iniciativa e controlo por humanos;
- Privacidade e fiabilidade dos dados;
- Transparência;
- Diversidade, não discriminação;
- Promover o bem-estar;
- Prever mecanismos de responsabilização;

2º fase: piloto;
3º fase: com confiança na ética e foco no ser humano, a IA serve o ser humano e não alguém que o vem substituir. Tentar promover uma uniformização entre o nacional e o internacional. Estão a ser desenvolvidos vários estudos.

Outras considerações

- Propriedade e acesso dos dados: *pode existir um direito e prioridade sobre os dados?* Fala-se sobre acesso aos dados e eventuais licenças compulsórias e obrigatórias para efeitos de acesso aos dados.
- Privacidade;
- Segurança: não só digital, mas também física;
- Propriedade intelectual: *o que acontece às obras produzidas por máquinas: protegidas por direitos de autor, objeto de patentes?*
- Consumidor: impactos vão ser tremendos. Quer as próprias diretivas, apesar de na proposta haver uma referência à internet das coisas, embora já não esteja lá presente.
- Contratos: regulam estas matéria.

Aula nº6 **24.10.2019**

Veículos autónomos

Helena Correia Mendonça
Marília Frias

Quer falemos de veículos autónomos terrestres quer falemos de veículos autónomos aéreos há ainda um vasto trabalho a percorrer, embora já exista alguma legislação quanto aos segundos.

Veículos autónomos e conectados

Evolução

- Falamos de autonomia e de concetividade. A ideia de um veículo sem pedais, sem volante, sem retrovisores é o culminar de um longo processo de desenvolvimento.
- Começou com *sistemas avançados de assistência ao condutor*: tem acesso, mas existem um conjunto de instrumentos que permitem auxiliar o condutor.
- Depois passamos à *conectividade*: desenvolvimento de um conjunto de regras para dar informação aos condutores na estrada;
- *Veículos autónomos e conectados*: já não falamos de mera assistência ao condutor, falamos de sistemas de condução autónomos; embora a autonomia não seja toda igual.
- *Mobilidade como serviço*: evolução no sentido de deixar de falar em automóvel como propriedade, mas antes como um serviço.

Conceito

Há 5 principais níveis de autonomia:

- Nível 0: não há tecnologia, nível básico; "puro aço";
- Níveis 1 e 2: assistência reduzida, avisos, notas aos condutores, barulhos do carro – ex: sinal de marcha-atrás;
- Nível 3: permite ao condutor não conduzir, mas em determinadas circunstâncias pode ser chamado a entrar na condução;
- Nível 4 e 5: *hands-off*; pode até nem haver condutor. O nível 4 é *hands off* mas só para alguns domínios, por exemplo, na autoestrada, dentro de Lisboa já não. O nível 5, por seu lado, é completamente *hands off*, o veículo anda por todo o lado sem necessidade de intervenção de um humano.

Conectado

- Os veículos autónomos têm de ter sensores para recolher informação à sua volta e também podem receber informação de outros veículos, pedestres, etc. não podemos ter autonomia sem conectividade.

Nações Unidas: UNECE, Comité dos transportes terrestres: Grupo de Trabalho > assegurar a segurança.

- Convenção de Genebra e a Convenção de Viena. As convecções dizem que o condutor deve estar presente para manobrar e controlar o veículo a qualquer altura, algo complexo de compatibilizar tendo em conta os níveis 4 e 5 de autonomia, especialmente com o nível 5.
- Proposta de revisão de março de 2014: ou o condutor consegue recuperar o controlo do veículo (dificuldades no nível 4 e 5), ou, não tomando o controlo, tem de estar de acordo com regras técnicas próprias para estes veículos.

WP1: *qual o nível de autonomia permitido pela alteração da Convenção de Viena?*

- Não existe uma opinião uniforme;
    - França: nenhuma das convenções permite nem nível 4 nem nível 5. Mesmo com as alterações efetuadas, para França ainda não conseguimos ter veículos de nível 4 e 5.
    - Reino Unido, Alemanha, Áustria, Espanha: entendem o condutor como o sistema autónomo e não o condutor humano.

Em todo o caso, os países concluíram que se existem dúvidas é necessário criar convenções, etc.

Quanto à utilização dos veículos

- Muito automatizados e totalmente automatizados: apesar de todas as dúvidas sobre esta possibilidade ou não, foram aprovadas algumas linhas orientadoras.
- Testes em ambiente real: tem de estar alguém próximo do veículo, não tem de ser o condutor, pode até ser um operador que o consiga controlar de alguma forma.

WP29: analisa temas puramente técnicos

- Acordo de 1958: regulamentos UN -120
- Acordo de 1998: UM GTR, Regulamentos técnicos globais – 20

Se queremos um veículo de nível 5 e se a Convenção de Viena diz que é necessário cumprir especificações técnicas criadas para estes veículos, há que perceber se ao abrigo destas regras temos normas suficientes para saber se se cumpre o requisito exigido pela Convenção de Viena.

- Acordo 1997: Regras da ONU
- Regulamento 79: alterado recentemente para sistemas avançados de direção de assistência ao condutor, excluindo os sistemas de direção autónomos (fora do âmbito de aplicação).

- Documento quadro sobre veículos autónomos, chamando a atenção para aspetos chave de segurança;
- Cibersegurança;

- Atualizações de software
    → transformarem-se nos regulamentos UM

Políticas da União Europeia

1. Comunicação
    - Mobilidade segura: *e-call*, segurança de veículos
2. Comunicação:
    - Há legislação europeia para ter veículos de nível 5, mas há que continuar a legislar.

Legislação

Homologação

- Regulamento 2018/858 (revoga a diretiva 46/2007/EC a partir de 1 de janeiro de 2020)
    - Regime para novas tecnologias e conceitos: para ter veículos com autonomia no mercado, entendem que se deve informar quais as características, segurança, testes e depois de analisado é dada uma resposta.
- Regulamento 661/2009: sobre segurança dos veículos
    - Nova proposta em cujo objetivo é refletir a autonomia dos veículos.

Infraestrutura rodoviária

- Diretiva 2008/96, 19 de novembro de 2008.
    - Vai ser revista para fazer frente aos veículos autónomos.
    - Os sistemas de sinalização dos veículos devem poder ser lidos pelos veículos autónomos.

Condutores: Diretiva 2006/126

- Condutor *vs* operador + requisitos;
- Examinadores
- Comportamento do condutor > código de estrada
- Trânsito do veículo.

Responsabilidade

⇒ Contraordenacional, civil e criminal.
    - Responsabilidade do condutor *vs* responsabilidade do sistema
    - Se o veículo estiver a ser conduzido pelo sistema analisamos a responsabilidade por produtos defeituosos.
    - Seguro obrigatório de veículos: o produtor do veículo deve ter? Não. Continua a ser o condutor a ter essa obrigação. Em caso de acidente a seguradora cobre o dano e depois tem direito de regresso por parte do produtor.

Sistemas de aeronaves não tripuladas

Terminologia

→Por detrás da regulamentação dos drones estão as questões de segurança.
→ A terminologia tem vindo a variar consoante os diplomas. Drone = RPAS= UAS

Legislação nacional

> Regulamento da ANAC, 2016

>
>
>

Regulamento nº1093/2016:

- Regras gerais:
- Regras especiais:

→ voanaboa.pt

Tudo o que sair destas regras requer autorização da ANAC.

DL 58/2018:

- Criou um sistema de registo do operador do drone;
- Seguro de responsabilidade civil: a aguardar uma portaria.

Legislação da União Europeia

- Regulamento 2018/1139: regulamento base; trata de todos os temos da aviação civil.
- Regulamento de execução: estabelece as regras sobre a operação dos drones
    - Categoria aberta: tem menos risco, drone mais leve em zonas de menos perigo.
        - Cumprem requisitos específicos;
    - Categoria específica: sujeita a licença de exploração; avaliação do risco e medidas mitigadoras, decisão da ANAC; emissão de um LUC- licença que permite fazer um vasto leque de operações. Cenários de referência: previsão do cenário, dispensa licença.
    - Categoria certificada: operações que implicam um risco mais alto, obriga-se a uma (...)
- Regulamento Delegado: tem mais a ver com a conceção e o fabrico das aeronaves.

Entidades mais relevantes

- ANAC
- AAN
- EASA

Os aviões quando andam no céu não o fazem de forma aleatória: há toda uma gestão do espaço aéreo. Neste momento, não existe nada no que toca ao uso do espaço pelos drones. Há um projeto de regulamento que ainda não é público. Com este novo diploma pretende-se regular a prestação de serviços de drones sem criar conflito. A ideia é combinar serviços de entidades privadas ou públicas.

U-Space

- Quadro de procedimentos e serviços específicos para o acesso ao espaço aéreo pelos drones. Há combinação perfeita entre a tecnologia e utilização desta por aeronaves não tripuladas.

Aula nº7 **31.10.2019**

Cibercrime

Beatriz Seabra de Brito

Porque é que o cibercrime é assim denominado e não como simplesmente crime? O que é que o caracteriza que implica a sua conceptualização como tipo autónomo?

Consiste num grupo autónomo de infrações penais com carácter sistemático; exigências metodológicas distintas ...

O cibercrime é, em primeira linha, crime. Ou seja, as condutas realizadas no ciberespaço são razão suficiente para serem tratadas de forma específica. A razão passa por ocorrerem num espaço distinto do espaço real.

William Gibson foi a primeira pessoa a introduzir o conceito de ciberespaço – 1982. O ciberespaço é na verdade um não espaço e hiperespaço, ou seja, ao mesmo tempo que é uma realidade paralela à do servidor; e hiperespaço (...)

Métrica do cibercrime

Funciona como um novo grupo de tipos incriminadores ou se reconduz a um tipo dos tradicionais tipos incriminadores, mas que ocorre num ambiente diverso? As soluções aplicáveis ao universo dos cibercrimes são exatamente as mesmas que se iriam aplicar ao crime físico-real, mas com adaptações.

A determinação das fronteiras daquilo que determina o cometimento de crimes através de sistemas de informação e o cometi (...)

Aquilo que é a determinação de uma realidade conceptual própria não é absolutamente evidente. A dificuldade reside na inexistência de uma definição consensual daquilo que é o cibercrime, além de se atribuir uma diversidade enorme de conceitos para definir o mesmo.

- Decalca de forma rigorosa a circunstância de ser cometido no ciberespaço;
- Os autores que tratam melhor do assunto também se reportam como cibercrime;
- A designação utilizada pela Convenção de Budapeste é antiga e há muitos aspetos não atuais, visto ser o primeiro instrumento internacional que trata destas temáticas. Não há lá definição de cibercrime, mas há a definição de *cyber space offenses*. Uma ofensa cometida no ciberespaço é aquela que é cometida por redes de telecomunicação. Decorre daqui que a definição que é apresentada considera que o cibercrime tem de ser mais do que um crime cometido através de redes de telecomunicação e nessa medida existem outras formas de cometer crimes que cabem no conceito de cibercrime.

→ Há uma lei do cibercrime – Lei nº109/2009 (disposições de direito penal material) - e não há definição sobre o seu conceito nem sobre o conceito de ciberespaço.

Cibercrime em sentido normativo: algumas definições

- Comissão Europeia: cometido online, através do uso de instrumentos de telecomunicação, de instrumentos informáticos;
- Departamento de justiça dos EUA:
    - Acrescenta coisas à definição apresentada pela CE - acrescenta que o cibercrime pode ter por objeto o sistema informático, através de meios informáticos.

-

- Não considera ser uma forma de cibercrime.

→ Segundo a CE, só o primeiro caso é que é cibercrime.

O cibercrime, apesar da dificuldade da sua definição, incorpora duas modalidades: por um lado, o sistema informático ou a internet deve ser utilizado como ferramenta; por outro, a internet ou o sistema informático pode ser utilizado como alvo.

Neste caso, o João não se serviu de nenhum dispostito eletrónico para cometer o crime que cometeu. O que o João fez integra o conceito de cibercrime?

- Art.4º LC: parece possível integrar o tipo incriminador aqui definido no ato de João, conceito lato de aproximação americana. Na opinião de Beatriz Seabra de Brito, o art.4º inclui danos relativos a programas ou a dados informáticos – definição de dados informáticos está definido na presente lei. Há uma certa redundância no titulo do artigo.

Fernando Miró Linares: introduz uma nova classificação de cibercrime. Diz que no universo de todos os cibercrimes há crimes cujo cometimento **só** é possível no ciberespaço e há outros que **podem** ser cometidos no ciberespaço – tipos incriminadores com existência no plano físico-real, mas também no plano do ciberespaço.

Exemplos:

- Cibercrime puro:
- Cibercrime réplica:
- Cibercrime de conteúdo: justifica-se porque muitos dos crimes tradicionais com réplica no espaço têm as suas características alteradas – ex: pornografia infantil. Se distribuir a alguém, o âmbito de visualização é mais pequeno do que se for difundido via internet.

Por que razão é o cibercrime cibercrime e não um crime?

1. Autonomia ontológica do ciberespaço:
    a. Significa que apesar de o ciberespaço estar dependente de uma realidade físico-real, a sua existência é autónoma, e implica alterações na sistemática do facto punível – modelo que os alemães impuseram para determinar os passos de análise a uma conduta com relevância penal. O entendimento de Beatriz Seabra de Brito incide sobre a existência de duas categorias: tempo e espaço. A circunstância de nós no ciberespaço termos um hiperespaço e aquilo que implica que o conceito de ação seja a primeira categoria do facto punível tenha de sofrer uma alteração.
2. Características fundamentais dessa afetação:
    a. Os crimes cometidos no ciberespaço podem ser cometidos instantaneamente – clic que se replica de imediato no ciberespaço, algo que é mais moroso no espaço físico.

Conclusões

- O cibercrime é crime: existem as mesmas características essenciais entre o crime cometido no espaço físico-real e o crime cometido no ciberespaço. Devem ser valorados como condutas jurídico-penalmente relevantes se colocarem em risco bens jurídicos essenciais.

- Têm uma realidade própria e essa implica a consideração dos cibercrimes como um grupo de incriminações próprias que carecem de (...) esta autonomia decorre da circunstância dos fenómenos espaço e tempo serem próprios e distintos no ciberespaço.

Aula nº8 **07.11.2019**

Proteção de dados

Graça Canto Moniz

Os algoritmos e o titular dos dados: que proteção?

O titular dos dados é quem é protegido pelo RGDP, quem é titular do direito fundamental à proteção de dados. No âmbito da UE, nós temos dois direitos: direito à reserva da intimidade da vida privada e o direito fundamental à proteção de dados.

Discussão sobre o episódio *Hang the DJ* da série *Black Mirror*

→ O algoritmo é quem decide.

Como é que nós, sem deixarmos de fazer parte da maneira como a sociedade funciona - digital – nos conseguimos proteger neste ambiente? Se é que nos consigamos proteger.

Dignidade da pessoa humana – restringe direitos de autonomia; não há uma verdadeira autonomia, mas sim uma sujeição, limita a liberdade e a privacidade.

Os algoritmos são esquemas automáticos e matemáticos que tomam conta das nossas vidas, isto tudo independentemente da vontade das pessoas em manter ou não aquela relação. É aqui que entra o direito do titular dos dados.

Direitos propostos pelo RGPD

- Direito de resposta;
- Direito a ser informado;
- Direito de acesso;
- Direito de ratificação, ao apagamento;
- Direito de limitação do tratamento;
- Direito de portabilidade;
- Direito de oposição;
- Direito específico para decisões individuais e automatizadas.

O direito ao esquecimento, embora tenha a mesma epígrafe do direito ao apagamento, foi reconhecido por uma decisão do TJUE: estava em causa um pedido de um cidadão espanhol a pedir a desassociação do seu nome a um link em relação a uma dívida. Como entendeu que a sua imagem digital não estava salvaguardada uma vez que até já tinha saldado a dívida, decidiu pedir para ser esquecido. Se escrevermos o nome do senhor no motor de busca já não encontramos a referência, embora a notícia permaneça na fonte original, no jornal La Guardía.

Estrutura do art.22º RGPD

Só estão abrangidos tratamento automatizados. Ou seja, não é verdadeiramente um direito, mas sim uma proibição dirigida às empresas e às entidades públicas. Contudo, existem exceções elencadas no nº2: consentimento explícito – o titular dos dados tem de ser informado da recolha de dados e do modo como isso será feito.

Mas há ainda proteção do titular nos casos em que não concorde com o perfil definido pelo algoritmo. Tem direito a obter intervenção humana no processo decisório; pode demonstrar o seu ponto de vista e pode ainda contestar a decisão. Todos estes direitos não estavam previstos no episódio da série.

Importa ter presente que estes direitos são exercidos no momento em que há tratamento dos dados e onde já há uma decisão.

Decisão recente (abril de 2019)

- Instituição financeira com software com base no algoritmo decidia se certa pessoa era ou não suscetível de ter um crédito bancário.

Críticas da doutrina ao art.22º

- O legislador poderia ter ido mais longe.
- Âmbito de aplicação: aplica-se a um número muito reduzido de casos; G29: a intervenção humana tem de ser significativa, tendo um impacto também significativo na decisão.
- Interpretação: "produção de efeitos jurídicos na esfera jurídica". G29: estas duas expressões acontecem quando o estatuto jurídico da pessoa ou os seus direitos no contrato são afetados.
- Eficácia das faculdades do titular dos dados: o RGPD não esclarece quais são os efeitos da contestação que o titular dos dados faz à decisão com base nos resultados do algoritmo. O que acontece se existir discordância entre a entidade e o titular dos dados? Era útil que o titular dos dados conhecesse a mecânica do processo, contudo, isso pode ser um grande desafio para o cidadão comum. Estas limitações não significam que o titular dos dados está totalmente desprotegido. Isto porque toda a lógica do RGPD está assente na prevenção de riscos: desde o momento da sua entrada em vigor todas as entidades publicas devem cumprir as suas diretrizes. Há que fazer uma avaliação do impacto do tratamento dos dados pessoais de modo a medir o risco que isso coloca aos titulares dos dados. A natureza regulatória do RGPD encontra-se subordinada à ideia de prevenção do risco do tratamento dos dados pessoais (art.4º RGPD). A proteção do titular é preventiva, pelo que o tratamento é antecedido por dois momentos: avaliação do impacto, e na sequência desta contactar com a autoridade responsável; medidas adotas ao abrigo da proteção de dados desde a conceção.
- Proteção de dados desde a conceção (art.25º): definição dos meios de tratamento no momento do próprio tratamento. Antes do algoritmo tomar qualquer decisão, o responsável pelo tratamento tem de respeitar estas obrigações definidas no referido artigo. Não pode recorrer a um algoritmo que não lhe permita cumprir com o art.25º.
- Avaliação de impacto: é obrigatório e por isso tem de ser realizada. Há uma espécie de auditoria prévia que pode ter como consequência uma consulta à Comissão Nacional de Proteção de Dados, autoridade de controlo.

Conclusões

- Admitindo-se que o art.22º tem algumas limitações, nomeadamente em relação às faculdades que nos reconhece, há garantias que as entidades têm de cumprir pelo respeito ao RGPD. Estas garantias não substituem a intenção legislativa de promover a transparência algorítmica ou de corrigir situações nas quais o ser humano está subordinado à máquina. Por um lado, contribuem para prevenir danos no titular dos dados, mas procura também um contributo de proteção da dignidade e evitar a

subordinação do Homem à máquina. Obriga as organizações a terem estas diligências antes do tratamento dos dados.

Ex: pseudonimizar: substituição do nome pelo número, e depois ficava fechado num anexo e lia-se 1,2,3 é casada e tem 4 filhos. Anonimização: há quem garante que isso não é possível. A encriptação caberia no meio destas duas.

→ protecaodedadosue.cedis.fd.unl.pt

Aula nº9 **14.11.2019**

Big data, internet of things e contratos

Jorge Morais Carvalho

Big data

Conceito

Rápida recolha, armazenamento e tratamento automatizado de um conjunto enorme e variado de dados.

Nos últimos dois anos foram criados tantos dados como em toda a história da humanidade antes destes dois anos.

A grande questão e o que os torna relevantes são aqueles três primeiros aspetos: rápida recolha, armazenamento e tratamento automatizado. Foi isto que permitiu a evolução tecnológica nos últimos anos. Ex: cloud

Ideia principal: permite uma cada vez maior personalização da oferta de bens e serviços. A oferta, há anos atrás, era completamente estandardizada, embora não estivesse dirigida a uma determinada pessoa. Hoje, com esta grande quantidade de dados que são tratados, é possível personalizar a oferta em específico para uma pessoa e não para um conjunto de pessoas.

Utilização

- Informação introduzida pelos trabalhadores, consciente ou inconscientemente.
    - Espaço e tempo são informações também recolhidas. Há anos atrás, estes dados não eram transmitidos, nem tão pouco eram criados. Criamos mais dados hoje porque temos computadores, telemóveis com conexão à internet. OS smartwatches não tiveram assim tanto impacto, embora a sua proximidade com o individuo seja maior porque esta no pulso, permitindo o tratamento de informação interna, como a pulsação.
- Através de dispositivos variados (computadores, smartphones, wearables, smartwatches)
- De diversas formas: navegação, pesquisas, utilização de programas e aplicações, comportamento nas redes sociais, etc.
- Toda esta informação pode ser relacionada com o espaço (localziaçao do utilizadot) e com o tempo (dia, hora).

Vantagem para o utilizador de *big data*

Tratamento totalmente automatizado, sendo os modelos de análise construídos por algoritmos.

Permite com uma exatidão nunca antes conseguida, antecipar o comportamento de pessoas que correspondem a determinadas características e, com base em dados a elas relativos, orientar a informação transmitida.

E para o destinatário da oferta?

Acesso a informação orientada aos seus interesses. Mas eventual exploração de fragilidades.

Problemas:

Por exemplo, o Facebook já mostrou conseguir influenciar as eleições nos EUA entre 1% e 2% (ou 6%).

Há uma tendência para fazer uma associação de interesses entre as pessoas, não por maldade, mas por achar que é o que vai interessar mais àquela pessoa. Ao contrário do que acontece com o conteúdo televiso que é independente dos interesses das pessoas e tenta abranger todas as gerações. Ainda assim, somos influenciados desde sempre, mesmo que o conteúdo não seja direcionado para os nossos interesses, acabam por criar uma certa necessidade no espetador que inicialmente este não tinha.

Personalização das condições contratuais

Posso tirar ao mesmo tempo de um mesmo site um bem e cujas condições são diferentes.

- Proposta contratual dirigida à pessoa A relativa a um determinado bem ou serviço pode ter cláusulas diferentes da proposta dirigida, quanto ao mesmo bem ou serviço, à pessoa B, por se saber que aquela tem tendencialmente mais interesse em celebrar o contrato.
- Quando A abre a página, o relógio custa € 150. Quando B abre a página, o relógio custa € 100. É possível?
- Diferenciação do preço? Do ponto de vista técnico é possível, mas de um ponto de vista contratual, jurídico é possível? Uma norma imperativa tem de ter uma razão de ser, sem justificação para isso deve concluir-se que não é uma norma imperativa. Diferença entre fixação de preço dinâmica e fixação de preço personalizado.

No caso das viagens de avião online, há uma clara ilegalidade porque o preço contratualizado é diferente do preço a pagar, existindo um problema de informação.

Neste caso em concreto, as pessoas sabem o preço. Com esta personalização de bens e serviços já não estamos perante propostas ao publico, estamos perante uma proposta dirigida a uma pessoa determinada.

Diretiva – Modernização

Considerando (45): "Os profissionais podem personalizar o preço das suas ofertas para consumidores específicos ou categorias específicas de consumidores, com base em decisões automatizadas e na definição de perfis de comportamento dos consumidores, de molde a permitir-lhes avaliar o poder de compra do consumidor. (...) Os consumidores deverão ser claramente informados sempre que lhes seja apresentado um preço personalizado com base numa decisão automatizada, de modo a poderem ter em conta os potenciais riscos nas suas decisões de compra. (...) Esta obrigação de informação não se deverá aplicar a técnicas como a tarifação dinâmica ou em tempo real, que implica a alteração dos preços de uma forma extremamente flexível e rápida em resposta às exigências do mercado, quando essas técnicas não envolverem uma personalização com base em decisões automatizadas".

Portanto, respondendo à questão anterior, podem. Mas os consumidores deverão ser claramente informados. La está, tem de haver informação de que aquela oferta é personalizada, não pode ser induzido em erro no sentido de considerar que aquela proposta é automatizada e igual a todos os clientes, se for caso disso.

Personalização de bens e serviços

- Quando A abre a página, aparece uma camisola do Benfica, clube de A, com o número 1970 nas costas (ano de nascimento de A).
- Quando B abre a mesma página, aparece uma camisola do Belenenses com o número 1976.

Contratação associada a análise de riscos

- Análise de risco pode ser feita de forma cada vez mais individualizada.
- Exemplos: contratos de crédito; contratos de seguro.

É especialmente relevante o tratamento de big data.

Vantagens e desvantagens?

- Por exemplo, um banco pode recusar-se a conceder crédito. Outro exemplo, o banco recusou-se a conceder um crédito a um senhor porque não tinha dados suficientes sobre o seu histórico.

Internet of things

Conceito

Ligação das coisas à internet, garantindo uma gestão inteligente dessas coisas. Aqui, a palavra chave é automatização.

É um instrumento poderoso, pela ligação aos big data (transmissão e tartaento automatizados da informação).

Exemplo

Frigorífico inteligente que, tendo a informação de que já só há um iogurte, contacta diretamente um supermercado *online*, encomendando mais iogurtes.

Contrato entre coisas? As coisas são partes de um contrato?

Não.

Como cumprir as normas legais relativas ao dever de informação?

São transmitidos de forma automática, se calhar até de forma mais eficaz, e não cai na tentação de comprar mais do que aquilo que preciso uma vez que o próprio frigorifico responsabiliza-se por essa tarefa.

DL 7/2004 Comércio eletrónico

- 1 - À contratação celebrada exclusivamente por meio de computadores, sem intervenção humana, é aplicável o regime comum, salvo quando este pressupuser uma atuação.
- 2 - São aplicáveis as disposições sobre erro:
    a) Na formação da vontade, se houver erro de programação;
    b) Na declaração, se houver defeito de funcionamento da máquina;

c) Na transmissão, se a mensagem chegar deformada ao seu destino.

- 3 - A outra parte não pode opor-se à impugnação por erro sempre que lhe fosse exigível que dele se apercebesse, nomeadamente pelo uso de dispositivos de deteção de erros de introdução.

→ Não havia referência há contratação celebrada exclusivamente através de instrumentos eletrónicos.

Novamente os contratos de seguro

- Revolução na análise de comportamentos.
- O carro pode ter um computador que avalie a quantidade – UBI (*Usage Based Insurance*) – e a qualidade – PHYD (*Pay How You Drive*) da circulação, com impacto no preço a pagar pelo tomador do seguro.
- Noutros ramos, a utilização de um dispositivo que permita monitorizar a atividade e o ritmo cardíaco do segurado pode também implicar alterações do preço (ou até ser imposta para a contratação).

Smart contracts

Conceito

Contratos sem intervenção humana no momento do cumprimento, que se executam automaticamente através de códigos de programação (que reproduzem linguagem jurídica).

Não é uma novidade do ponto de vista conceptual (*vending machines*), mas a evolução tecnológica permite uma utilização em novos domínios (graças à redação de contratos em linguagem de programação e à utilização da tecnologia *blockchain*).

O programa tem controlo sobre os bens (físicos ou digitais) que são objeto do contrato (e, portanto, que devem ser prestados).

Vantagem: executam-se automaticamente

Não são novidade do ponto de vista conceptual. Há mutito anos que existem as vending machines. A grande diferença é que a evolução tecnológica permite o aumento exponencial da programação de contratos e utilização da tecnologia blockchain por outro.

O programa tem controlo sobre os bens que são objeto do contrato.

Exemplo

- Contrato de aluguer de um automóvel (um ano, com prestações mensais de X bitcoins).
- *If*… o valor monetário não for pago (verificação automática numa blockchain);
- *Then*… o carro deixa de andar.

Problema

Conceitos indeterminados. No direito temos de aplicar muitos conceitos indeterminados.

- Locatário paga apenas uma parte do preço, uma vez que entende que o carro não está a funcionar em conformidade com o que ficou estabelecido no contrato. Como programar esta situação?
    - Como programar um defeito? Uma desconformidade? Ou como é que se programa a boa fé?

Aula nº10 **21.11.2019**

Plataformas digitais

Jorge Morais Carvalho e Joana Campos Carvalho

Grande parte dos bens e serviços que adquiríamos de forma dita tradicional, passamos a aceder a eles através de plataformas digitais.

Nem sempre que uma empresa se apresenta como uma plataforma aliás, pode ser uma intermediária. Dentro daquelas que são plataformas, como se tratará a questão da responsabilidade civil?

O que é uma plataforma?

Começou a ser estudado na área da economia e os juristas adotaram-no e adaptaram-no às suas necessidades. Em termos económicos são mercados bilaterais ou multilaterais. Servem como intermediarias entre dois ou mais grupos de utilizadores que estão ligados por efeitos de rede indiretos.

Efeitos de rede indiretos: O valor que um participante retira da utilização da plataforma aumenta em função do número de participantes do outro grupo.

Em todas as plataformas existem sempre efeitos de rede indiretos que ligam dois grupos de utilizadores, o que implica que o valor que um dos participantes retira esta diretamente ligado ao número de utilizadores do outro lado. Ex: encontrar hotel em Paris – Booking – disponibiliza 5 hotéis, portanto, a utilidade retirada é reduzida, se compararmos com uma outra cidade que nos ofereça 500 unidades hoteleiras. Como os dois lados estão ligados, há necessidade de fazer ambos crescer.

Em todas há uma triangularidade: existe o operador da plataforma sempre, que serve de intermediário entre o fornecedor e o cliente.

Plataformas digitais: as redes sociais são plataformas digitais, não são bilaterais, são sim multilaterais porque temos um conjunto de utilizadores que interagem entre si, embora permaneça a ideia da triangularidade e dos efeitos indiretos. Os jogos online também são plataformas digitais; sites de encontros, listings, classificados online, plataformas que permitem a celebração de contratos.

Mercados em linha

Plataformas que permitem que as pessoas celebrem contratos entre si ou que permitem que as pessoas encontrem uma contraparte para o seu contrato. Por exemplo, o Facebook não é só uma plataforma digital mas também é market place, por permitir o encontro com pessoas.

O operador de mercado em linha será um intermediário entre os dois grupos de utilizadores, entre as partes do contrato principal.

Modelo de contratação tradicional

Relação entre duas pessoas, duas partes.

Modelo de contratação nas plataformas

Deixamos de ter uma linha e duas pessoas e passamos a ter uma estrutura triangular. Para cada contrato principal, existem mais dois contratos associados: olhando para o mercado em linha, constatamos que existe uma relação entre o intermediário da plataforma e o fornecedor – que serviços a plataforma vai prestar, por exemplo -, intermediário e o cliente – regular os termos nos quais o cliente vai utilizar a plataforma digital -, fornecedor e o cliente – contrato principal, é o que na estrutura tradicional consistiria no único contrato celebrado; para que este ocorra numa plataforma digital, existem mais dois contratos associados.

As lojas online de determinada marca normalmente não são plataformas digitais (Ex: site da Zara, o contrato é diretamente com a Zara e não temos uma plataforma, o contrato é celebrado nos termos do contrato celebrado offline). Há que olhar para o modelo negocial para perceber em que é que consiste a plataforma.

Triangularidade aparente

Para as plataformas poderá ser interessante mostrar que estão a colaborar, ou mostrar apenas esta relação de triangularidade, mas no que respeita ao contrato entre o fornecedor e o cliente, a plataforma pode dizer que não é responsável pelo contrato principal. E há casos em que não existe uma plataforma.

Caso da Uber

Com quem é que contratamos? Que contratos são celebrados no caso da utilização da aplicação da Uber?

A plataforma como intermediário:

- Uber contrato com motorista,
- Uber e passageiro,
- Motorista e o passageiro (contrato de transporte).

⇒ Basicamente, a plataforma está a desresponsabilizar-se em caso de algo correr mal.

TVDE: transporte em veículo descaracterizado em plataforma eletrónica. TVDE é um prestador de serviços, que tem diversos motoristas que depois são direcionados para as várias empresas de deslocação, como Uber, Bolt ou Kapten.

- Todas as interações do passageiro são com a Uber (celebração do contrato na aplicação, cobrança do preço).
- A qualidade está associada à marca.
- Não há escolha do motorista (só é apresentado depois de concluído o contrato).
    - Aqui, sendo a Uber parte, é responsável. A questão da responsabilidade só é suscitada no caso de haver uma efetiva triangularidade, em que a plataforma não é parte no contrato principal.
    - No momento da celebração do contrato, um declaratário normal está convencido de que está a celebrar um contrato com a Uber e não com o motorista X.

Direito Europeu

- Acórdão do TJUE, de 20/12/2017 (Proc. C-434/15, Acórdão Asociación Profesional Elite Taxi).

- "(…) há que considerar que este serviço de intermediação faz parte integrante de um serviço global cujo elemento principal é um serviço de transporte e, portanto, corresponde à qualificação, não de «serviço da sociedade da informação» (…), mas sim de «serviço no domínio dos transportes» (…)".

"Meras intermediárias"
Responsabilidade da plataforma

Três contratos

1. Contrato entre o fornecedor e a plataforma;
2. Contrato entre o utilizador e a plataforma;
3. Contrato principal entre o fornecedor e o utilizador.

Se algo corre mal no contrato principal, a plataforma pode ser chamada a responder? Quem é responsável pelo (in)cumprimento do contrato principal? Apenas as partes ou também a plataforma?

Exemplo: A Maria decidiu ir passar uma semana ao Algarve. Encontrou uma casa no Airbnb que era perfeita: 3 quartos para acomodar a família toda, piscina e a 2 minutos a pé da praia. Quando chegou, percebeu que afinal a casa era um T1 sem jardim e a 30 minutos a pé da praia.

Pode responsabilizar-se o fornecedor, mas de alguma forma podemos responsabilizar a plataforma?

- Não interessa o que a plataforma nos diz nos seus termos e condições. "A plataforma não é responsável por nada do que aconteça no contrato principal".
- É sempre necessário analisar a solução concreta para concluir quem celebra o contrato principal.
- Se for o próprio "operado da plataforma" a questão fica resolvida.
- Podemos chegar à conclusão de que nem sequer estamos perante uma verdadeira triangularidade. Se concluirmos que há uma triangularidade, então é preciso ver se se justifica haver algum tipo de responsabilidade.
- Os graus de intervenção variam: há que as analisar pelo modelo de negócio que efetivamente têm.
- Se as plataformas conseguissem levar avante a questão de não serem responsabilizadas, seriam apenas fonte de lucro. Mas na economia dos contratos, isto não faz sentido porque ao lucro está associado algum risco.

Intermediários?

- Plataformas são sempre apenas meros intermediários?
- Os graus de intervenção da plataforma variam bastante.
- Importância da questão: lucro sem risco?

O futuro

Não há uma verdadeira reposta, mas já existem progressos legislativos em relação a esta matéria.

- Diretiva europeia: não aborda nada sobre responsabilidade, mas fixa algumas obrigações para as plataformas e que têm de ser cumpridas: informar de que estão a celebrara um contrato com um terceiro, tendo também de informar acerca da qualidade ou não do profissionalismo da outra parte – abordar direito do consumo. As plataformas não podem simplesmente ter um modelo de negócio totalmente isento de obrigações e deveres, optando por consagrar algumas obrigações.
    - *New Deal for Consumers* - Proposta de Diretiva para melhorar proteção dos consumidores:
        - ... o prestador do mercado em linha deve fornecer as seguintes informações:
        - (a) Principais parâmetros que determinam a classificação das propostas apresentadas ao consumidor em resultado da sua pesquisa no mercado em linha;
        - (b) O facto de o terceiro que oferece os produtos, serviços ou conteúdos digitais ser ou não um profissional.

- Grupo de Investigação do *European Law Institute*: preparou uma proposta de lei modelo sobre plataformas digitais – ELI model rules on online platforms- , é meramente académico, embora não tenha relevância jurídica. Sendo que aqui já se aborda o tema da responsabilidade. As plataformas são conjuntamente reesposáveis com o fornecedor sempre que há incumprimento do contrato principal, sem prejuízo de direito de regresso, sempre que a plataforma controlar o fornecedor – critérios. A ideia é, quando alguns destes critérios estejam preenchidos, sendo o tribunal a avaliar, se a plataforma for tão poderosa de tal modo que influencie o contrato principal, então deverá ser responsabilizada.
    - Art. 11.º/1+16.º - dever de informar que o contrato é celebrado com um terceiro.
    - Art. 11.º/3+16.º - dever de informar sobre a (não) aplicação do direito do consumo.
    - Art. 17.º - Dever de eliminar informação enganadora da plataforma quando é notificada.
    - Art. 18.º - Responsabilidade (conjunta com o fornecedor) pelo incumprimento do contrato principal quando a plataforma controla o fornecedor.
    - Direito de regresso.

Controlo sobre o fornecedor

- Critério do controlo da plataforma sobre o fornecedor:
    - Os termos do contrato principal são definidos pela plataforma (cláusulas contratuais gerais).
    - O preço é determinado pela plataforma.
    - A plataforma tem a possibilidade de reter pagamentos.
    - A publicidade é focada na plataforma e na marca e não nos fornecedores individuais.

Reviews e comentários

Mecanismos de controlo da reputação

Aquela pontuação que nos aparece é um elemento decisivo. Há uma lei que regula as estrelas de um hotel, sendo que a classificação na Booking é distinta, por exemplo, posso ter um hotel de 3 estrelas e uma pontuação de 7,8 e um hotel de 4 estrelas com 6,4. Isto terá impacto na escolha do consumidor.
Muitas plataformas utilizam mecanismos de *review* e comentários.

- Vantagens para o utilizador:
    1. Dispõe de informação valiosa no momento de contratar. É confiável? Adequa-se às minhas necessidades?
    2. Risco de uma má avaliação é um fator de pressão muito forte. Fornecedor irá procurar resolver o melhor possível eventuais problemas para evitar uma má avaliação que pode condicionar o futuro do seu negócio.

Problema

Veracidade da informação (reviews falsos, manipulação da informação).

Exemplo: *The shed at Dulwich* - chegou ao primeiro lugar do Trip Advisor e não existe. O objetivo foi demonstrar a fácil falsificação e manipulação do sistema.

Diretiva -modernização – Considrando 47

- Informar os consumidores se se aplicam processos ou procedimentos que assegurem que as avaliações são publicadas por consumidores que utilizaram ou adquiriram efetivamente os produtos.
- Dar a conhecer a forma como são efetuadas as verificações e prestar informações claras aos consumidores sobre o tratamento dado às avaliações, como, por exemplo, se todas as avaliações, positivas ou negativas, são publicadas, ou se essas avaliações foram patrocinadas ou influenciadas por uma relação contratual com um profissional.
- Prática comercial desleal induzir os consumidores em erro, declarando que as avaliações de um produto são apresentadas por consumidores que o utilizaram ou adquiriram efetivamente, quando não tenham sido tomadas medidas razoáveis e proporcionadas para garantir que essas avaliações são efetivamente publicadas por esses consumidores

⇒ **Resultados de pesquisas**: "Informações gerais (…) sobre os principais parâmetros que determinam a classificação (…) das propostas apresentadas ao consumidor em resultado da pesquisa e a importância relativa desses parâmetros em comparação com outros parâmetros" [art. 6.º-A-1-a) da Diretiva 2011/83/UE].

Aula nº11 **28.11.2019**

Proteção do consumidor de conteúdos e serviços digitais

Jorge Morais Carvalho

Exemplo:
Netflix: contrato de conteúdo e serviços digital.

- Que direitos é que temos relativamente ao objeto em causa? Defende-se que tem de haver um direito de propriedade. Quem compra um DVD com o *office* tem de ser protegido relativamente à titularidade do mesmo assim como uma pessoa que descarrega online, sendo que do ponto de vista material é a mesma coisa.

Apresentação

- Diretiva 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais processo legislativo longo e trata dos contratos de fornecimento de conteúdo e serviços digitais.
- Diretiva de harmonização máxima (art.4º) – os Estados não podem proteger mais.
    - Transposição: 1 de julho de 2021,
    - Entrada em vigor: 1 de janeiro de 2022
- É um complemento à diretiva 2019/771, não coincidindo o seu âmbito de aplicação.
- Complementa a Diretiva 2011/83 UE (requisitos de informação, entrega, transferência do risco).
    - dois regimes de conformidade - um para as coisas, outra para conteúdos e serviços digitais, não são aplicáveis ao mesmo objeto, podendo ainda assim ser aplicadas em simultâneo.
- Aplicação: normas devem aplicar-se apenas aos contratos celebrados após o início da vigência do diploma em causa.

Âmbito de aplicação

Âmbito de aplicação subjetivo

- Visam proteger o consumidor/profissional
- Só se o conteúdo não for utilizado por profissionais é que se aplica esta diretiva.
- Consumidor: "pessoa singular que (…) atue com fins que não se incluam no âmbito da atividade comercial, empresarial, artesanal ou profissional" [art. 2.º-6)]

Âmbito de aplicação objetivo

- Contratos de fornecimento e conteúdos ou de serviços digitais (art.3º/1) Novidades: aplica-se não apenas a contratos que tenham como contraprestação o preço, mas também a contratos de fornecimento de conteúdos ou serviços digitais que tenham como contraprestação dados pessoais.
    - Contrapartida:
        - Preço ou
        - Dados pessoais.
- Liberdade dos Estados-membros no que respeita à determinação da natureza jurídica destes contratos:
    - Os Estados-Membros são livres, desde que as regras sejam cumpridas independentemente da qualificação jurídica.
- Aplicável a conteúdos ou serviços digitais desenvolvidos de acordo com as especificações do consumidor (art.3º/2).
    - Se alguém puder ser qualificado como consumidor e por exemplo pedir a um profissional para criar uma *app* para si continua a ser-lhe aplicável.
- Aplica-se a qualquer suporte material utilizado exclusivamente como meio de disponibilização dos conteúdos digitais (art.3º/3).
    - Ex: cartão FNAC Netflix, por exemplo; CD; DVD; PEN.
- Não é aplicável a conteúdos ou serviços digitais que estejam incorporados em bens ou com eles estejam interligados (art.3º/4) – diretiva de consumo.

- Os bens têm elementos digitais – por exemplo: computador, carro. O critério será a predominância – o que é que é mais relevante o bem ou o serviço digital e o bem é secundário? É aqui que surge a questão da box.

Classificações principais

- Conteúdos digitais / Serviços digitais
- Um ato único de fornecimento ou uma série de atos individuais de fornecimento / Fornecimento contínuo durante um determinado período
  - Ex- contrato de fornecimento para ter o *office*; celebro um contrato pelo qual me é enviado mensalmente de forma digital o número de uma revista – isto é relevante para efeitos de prazo de garantia.
  - Fornecimento contínuo: Ex- Netflix.
- Fornecimento durante um determinado período (contínuo ou através de uma série de atos) / Um único ato de fornecimento

⇒ Alterações do contrato pelo profissional:

- Contratos instantâneos em que há um único ato de fornecimento.
- Contratos de fornecimento durante um determinado período (contínuo ou numa série de atos distintos).

Aplica-se a diretiva 2019/770?

- Contrato de compra e venda de uma camisola na Zara
  - Não.
  - Bem com elementos digitais: camisola com ligação à internet → diretiva de consumo. Aqui, o elemento digital está incorporado no bem, não predomina.
  - Serviço ligado ao bem: um bem com elementos digitais. Foi no único ato que foi celebrado o contrato. – Diretiva da venda de bens de consumo.
- Contrato de compra e venda de um carro num stand, com uma aplicação de GPS instalada, comprometendo-se o vendedor a fazer atualizações de software durante um ano.
  - Aqui são partes diferentes, há dois contratos diferentes: compra e venda do carro e contrato de prestação de serviço de um conteúdo digital.
- Contrato de compra e venda de um carro num stand, sem aplicação de GPS instalada, indo o consumidor depois à página da Tom Tom na Internet adquirir a última versão de uma aplicação
- Contrato celebrado com o iTunes para a aquisição de uma música.
  - Conteúdo digital.
- Contrato celebrado com a Netflix para acesso a conteúdos por tempo indeterminado, com pagamento mensal de um preço
  - Serviço digital.
- Contrato celebrado com o Facebook para a criação de uma página pessoal
  - O objeto do contrato é o acesso interativo àquela página. Ainda que não haja um preço, a contraprestação são dados pessoais. Aplica-se o regime.

Dados pessoais – O problema

- Direito da Proteção de Dados / Direito dos Contratos (e, em especial, na Europa Direito do Consumo.

- Dados como objeto contratual com valor económico – como qualificar o contrato "gratuito" (sem contraprestação em dinheiro), mas em que o consumidor tem de fornecer dados?
    - Não podemos classificar como gratuito o contrato que tenha como contraprestação oferecer dados pessoais.
    - O que é que acontece se se tirar o consentimento? Deixa-se de ter acesso? A solução deve ser equilibrada. A partir do momento em que é retirado o consentimento, a pessoa noa deve continuar a ter acesso aos conteúdos.
- Empresas solicitam dados durante o processo de celebração do contrato e geram dados enquanto os consumidores utilizam o bem ou serviço (ligação com a Internet das Coisas)

Dados e contratos de consumo

- Dados como parte do serviço (assistentes pessoais, motores de busca, redes socais).
    - Por definição os dados são um elemento essencial para o cumprimento do contrato.
- Dados como forma de determinar condições relativas ao contrato (personalização dos bens ou serviços; personalização do preço; condições de acesso ao mercado)
- Dados como forma de influenciar a decisão do consumidor (identificação de preferências e fragilidades)

Tratamento de dados

- Art.6º/1: Num contrato, quatro fundamentos de licitude principais
    - Tratamento baseado no consentimento,
    - Tratamento necessário para a execução do contrato;
    - Tratamento necessário para o cumprimento de uma obrigação legal;
    - Tratamento necessário para o efeito dos interesses legítimos.

Dados como contraprestação

⇒ "A presente diretiva é igualmente aplicável sempre que o profissional forneça ou se comprometa a fornecer conteúdos ou serviços digitais ao consumidor e o consumidor *faculte ou se comprometa a facultar dados pessoais ao profissional*, exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para fornecer os conteúdos ou serviços digitais em conformidade com a presente diretiva, ou para o profissional cumprir os requisitos legais a que está sujeito, não procedendo ao tratamento desses dados para quaisquer outros fins" (art. 3.º-1-2.º parágrafo)

Tratamento baseado no consentimento

- Art.4º/11 RGPD: "«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".
- Art.7º/4 RGPD: "Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

- Parece ser proibido o fornecimento de dados pessoais como contraprestação. Temos dois instrumentos de direito europeu que parecem incompatíveis entre si – um diz que para haver consentimento não tem de estar subordinado e por outro lado se não der consentimento não tenho acesso aos conteúdos.

Fornecimento de conteúdos e serviços digitais

Cumprimento do contrato

- Arts.5º/1 e 2: Fornecimento dos conteúdos ou serviços digitais ao consumidor
- Art.5º/1: Prazo estipulado (na ausência de acordo, "sem demora indevida).
- Art.12º/1: Ónus da prova "relativo à determinação do fornecimento (…) nos termos do artigo 5.º recai sobre o profissional"

Não fornecimento

- Art.11º/1: O profissional é responsável pelo não fornecimento.
- Art.13º: Possibilidade de resolução do contrato, (i) após ser concedido um prazo adicional para cumprir ao profissional ou, (ii) em situações limitadas, de imediato
  - É necessário colocar o devedor numa situação de mora e só em situações excecionais é que é possível resolver de imediato.

Critérios de conformidade

Categorias

- Materiais / jurídicos
- Subjetivos / objetivos

Critérios subjetivos

- As estipulações especificamente acordados são parte do contrato.
- Utilização específica acordada entre as partes.
- Disponibilização das atualizações acordadas entre as partes.
- Acessórios, instruções e apoio ao cliente definidos no contrato.
- Caraterísticas resultantes de versões de teste ou pré-visualizações disponibilizados ao consumidor.

Critérios objetivos

- Utilizações habituais
- Características expectáveis tendo em conta a natureza do bem
- Fornecimento dos acessórios e instruções *expectáveis*
- Caraterísticas *expectáveis* tendo em conta as declarações públicas do vendedor ou de outras pessoas em fases anteriores da cadeia, como o produtor (publicidade e rotulagem)

⇒ Os subjetivos resultam do acordo entre as partes e os objetivos pressupõem razoabilidade, o que é compreensível tendo em conta a natureza do bem.

Características estipuladas

- Descrição
- Tipo*
- Quantidade

- Qualidade
- Funcionalidade
- Compatibilidade
- Interoperabilidade
- Demais caraterísticas (tal como exigidas pelo contrato).

Utilização específica

- Comunicada pelo consumidor ao profissional até ao momento da celebração do contrato
- Profissional tenha manifestado a sua concordância
- Ou seja: existe acordo quanto à finalidade específica

Caraterísticas tendo em conta a natureza do objeto e as declarações públicas

- Quantidade
- Qualidade
- Características de desempenho / continuidade
- Funcionalidade
- Compatibilidade;
- Acessibilidade;
- Segurança
    - Ex: compro um cd e tem um vírus – acontece que transmite vírus para o meu computador e para outros.

⇒ Critério de razoabilidade: desempenho de continuidade. O conteúdo tem de estar em conformidade com o contrato não apenas no momento em que é celebrado, mas também durante o tempo da execução do contrato e do fornecimento do serviço em si.

Fornecimento de atualizações

- Um único fornecimento (ou vários individuais): durante o período que o consumidor pode razoavelmente esperar dado o tipo e finalidade dos bens e dos elementos digitais, conteúdos ou serviços digitais, e tendo em consideração as circunstâncias e natureza do contrato.
- Fornecimento contínuo, art.10º/2 (Diretiva de bens de consumo), do conteúdo ou serviço digital durante um determinado período: durante esse período (no caso de bens com elementos digitais, esse período não pode ser inferior a dois anos.
    - Se houver fornecimento contínuo de um determinado serviço e se se tratar de um bem com elementos digitais nunca pode esse período ser inferior a dois anos. Não pode ser fornecido um computador com um sistema operativo e o profissional compromete-se a fazer atualizações durante 1 ano – não pode.

Instalação das atualizações

- É um ónus do consumidor. – Obsolescência programada.
- Vendedor não responde pela desconformidade resultante da falta de atualização, desde que (i) o profissional tenha informado o consumidor sobre a disponibilidade da atualização e as consequências da sua não instalação; e (ii) a não instalação ou a instalação incorreta da atualização pelo consumidor não se tenha ficado a dever a deficiências nas instruções de instalação.

Versão dos conteúdos digitais ou serviços digitais – art.8º/6

- Versão mais recente disponível
- Partes podem acordar o fornecimento de uma versão mais antiga

Integração incorreta

- Integração dos conteúdos e serviços digitais no ambiente digital do consumidor
- Consequência: falta de conformidade, (i) se fizer parte do contrato e tiver sido feita pelo profissional ou sob sua responsabilidade (ou pelo fornecedor dos conteúdos ou serviços digitais, no caso de bens com elementos digitais), ou (ii) pelo consumidor, estando as instruções incorretas
    - Elemento imputável ao consumidor.

Responsabilidade do profissional

Prazo

- Art.11º/2 e 3: Responsabilidade por falta de conformidade que exista no momento do fornecimento, distinguindo-se, quanto à sua manifestação, os casos em que se estipule.
    - (i) um único ato de fornecimento ou uma série de atos individuais de fornecimento – prazo facultativo (em alternativa, pode prever-se prazo de caducidade) mínimo de dois anos
    - (ii) o fornecimento contínuo durante um determinado período – profissional é sempre responsável dentro desse período

⇒ O fornecedor é responsável pela falta de conformidade que exista no ato de fornecimento.

Ónus da prova da anterioridade da falta de conformidade

- Art.12º/2: Ato único de fornecimento ou uma série de atos individuais de fornecimento – Profissional: prazo de um ano a contar do fornecimento
    - No primeiro ano, o profissional é que tem o ónus de provar que não havia qualquer inconformidade. Portanto, ao consumidor apenas basta alegar a falta de conformidade.

Direitos em caso de desconformidade

Elenco

- Reposição da conformidade
- Redução do preço
- Resolução o contrato

Hierarquia

- Hierarquia entre os direitos.
- Primeiro a reposição da conformidade (art. 14.º-2), não se distinguindo reparação e substituição.

Limites à imposição da reposição da conformidade

- Impossibilidade
- Custos desproporcionados

Requisitos relativos à reposição da conformidade

- A título gratuito,
- Num prazo razoável e
- Sem inconveniente importante para o consumidor
    - Conceitos indeterminados que têm de ser preenchidos no caso concreto.

Pressupostos para a redução do preço ou para a resolução do contrato

- Ausência de tentativa de reposição da conformidade
- Falta de conformidade apesar da tentativa de reposição da conformidade
- Gravidade da falta de conformidade
- Declaração (expressa ou tácita) de não reposição da conformidade pelo profissional

Efeitos da resolução do contrato

- O profissional deve reembolsar o consumidor do valor pago.
- Consumidor deve abster-se de utilizar os conteúdos ou serviços digitais e de os disponibilizar a terceiros.
    - Ex: Devolução do CD.

Prazo (de prescrição ou caducidade para o exercício de direitos)

Liberdade dada aos EM (art.11º)

- Não é obrigatório (exceto na ausência de prazo de responsabilidade do profissional)
- EM podem estabelecer os dois prazos ou apenas um deles (podendo, neste último caso, optar por qualquer um)
    - Desde que prevejam no mínimo aquele prazo de 2 anos. Combater a questão da obsolescência programada.

Alteração aos conteúdos e serviços digitais

Pressupostos para alteração unilateral

- Conteúdos ou serviços digitais fornecidos ou disponibilizados ao consumidor durante um determinado período.
- Previsão (i) *contratual* de uma (ii) *razão* (iii) *válida* para a alteração
- Alteração sem custos para o consumidor
- Notificação prévia de forma clara e compreensível
- Alterações com impacto negativo: informação sobre o direito de resolução ou de manutenção do objeto inalterado

Aula nº12 **05.12.2019**

Justiça e Tecnologia

Micael Martins Teixeira

Micael Martins Teixeira vê perigos em relação ao direito e à sua associação à tecnologia, mais até do que vantagens.

Advertências

- Direito é diferente de lei ou de política. A lei não é apresentada como sinónimo de Direito, mas sim como fonte de.
    - A lei é determinada em larga medida por razões/motivações políticas.

Não sendo o Direito lei, é o quê? Direito é a justiça no caso concreto. É uma atribuição de direitos. A justiça é, portanto, uma distribuição de direitos e deveres conforme a realidade do caso, não como lei.

Objeto: os perigos do uso de tecnologias para a determinação e aplicação do direito e os problemas que daí decorrem para a sociedade.

Direito e tecnologia: notícia "Honrar o legado do Freitas do Amaral", Mariana França Gouveia

- "Traduzir o pensamento jurídico em zeros e uns."

Exemplo 1 – tarifa social de eletricidade

- Regra hipotética: quem tem baixos rendimentos e baixa potencia contratada, pode beneficiar da tarifa social da eletricidade;
- Caso: certa pessoa tem rendimentos baixos, mas a potencia contratada é alta, apenas porque precisa da mesma para fazer funcionar uma cadeira-elevatória elétrica de que precisa para entrar em casa. Nesse sentido, foi-lhe recusado o pedido.
- A atribuição da tarifa social foi recentemente **automatizada**, não sendo necessário uma análise casuística para a sua atribuição (ou não atribuição); anteriormente carecia de requerimento. O sistema funciona agora em moldes semelhantes aos dos *smart contracts*.

Conclusões:

⇒ A **regra**, em **abstrato**, **é adequada e razoável**; e essa regra é facilmente aplicada por uma máquina;

⇒ Mas a **realidade é muito diversa**; uma regra, mesmo adequada e razoável, pode **produzir resultados injustos**;

⇒ A aplicação automática de uma regra **amplifica a injustiça** pois é totalmente insensível ao resultado da aplicação. A escolha de um método depende da justiça do resultado. Isto perde-se se for aplicada por uma máquina.

Exemplo 2 – COMPAS

→ *Correctional Offender Management Profiling for Alternative Sanctions* – software usado por alguns tribunais americanos que, usando alguns dados sobre o arguido, **calcula a probabilidade de reincidência criminal, fator que influência a pena**;

- Esta ferramenta assenta numa lógica probabilística, identificando fatores que apontam para maior probabilidade de reincidir, tais como:
    - Os pais do arguido separaram-se quando este era criança
    - O arguido tem amigos ou familiares que já praticaram crimes
    - O arguido já foi expulso da escola
    - O arguido tem dificuldades financeiras
    - O arguido é uma pessoa depressiva

⇒ É chocante o impacto e as consequências que estas tecnologias podem ter. Os objetos que estão na base destes programas funcionam.

Exemplo 3 – IA nas indústrias da banca e dos seguros

- Software inteligente (IA) é capaz de **estimar o risco de incumprimento de um mútuo bancário (banca) ou da ocorrência de um sinistro (seguros)**;
- Estes programas operam não só com base em critérios predefinidos, mas também com base em critérios que o próprio programa é capaz de estabelecer, identificando correlações entre certa característica e o incumprimento ou o sinistro *(machine learning);*
- Os programas não levam em conta apenas os dados diretamente relacionados com o «evento» (ocorrência passada de sinistros, montante do rendimento mensal), mas também muitos outros tipos de dados, tais como o histórico das pesquisas *online*, dados sobre compras *online*, atividade das redes sociais *(Big data).*
- Esta capacidade de identificar automaticamente novos fatores que indiciam a ocorrência de incumprimento ou do sinistro no futuro leva, potencialmente, a que o software identifique critérios como:
    - O «prestígio» da universidade em que se tirou o curso;
    - O risco de incumprimento ou de ocorrência de sinistros dos «amigos» das redes sociais;
    - A zona de residência;
    - A forma como a pessoa escreve (maiúsculas e erros ortográficos).

⇒ São critérios parvos, discriminatórios e irrazoáveis. Mas, uma vez mais, é verdade. Se um banco puder utilizar esta informação, consegue reduzir o número de pessoas que incumprem.

Conclusões

Ex: 2 e 3

- Não está em causa que estes desenvolvimentos tecnológicos permitem captar de forma muito abrangente certa parte da realidade, que **permitem prever**, com algum grau de **certeza**, **se certo arguido irá reincidir ou se certo mutuário irá incumprir o contrato;**
- *Qual é, então, o perigo?* É o **tratamento injustamente discriminatório** de quem é visado por estes programas informáticos;
- É injusto que alguém veja a sua pena aumentada por ter dificuldades financeiras ou que quem não estudou numa universidade de prestígio não obtenha, por essa razão, um empréstimo bancário;
- O fator "dificuldades financeiras" não está diretamente relacionado com a probabilidade de reincidência, nem a universidade em que se estudou com a probabilidade de incumprir o mútuo: é **uma correlação estatística e não uma causa objetiva no caso em análise**; a injustiça reside na falta de conformidade de tais fatores com a realidade do caso.
- Atenção: a **injustiça mantém-se** apesar de o uso deste software permitir reduzir o número de reincidências ou o número casos de incumprimento pelos mutuários!
- Estas **tecnologias** permitem **antecipar a realidade** com alguma eficácia, permitindo tomar decisões no pressuposto (normalmente verdadeiro) de que ela se irá manter: decidir aplicar uma pena mais grave a quem tiver dificuldades financeiras;
- A possibilidade de tomar decisões com essa informação favorece quem a tem;
- Ora, o **direito não visa a tomada de decisões** (ainda que para o bem comum, como seja minimizar a reincidência criminal) **com base no pressuposto de que a realidade se vai manter**; **o direito visa, precisamente, alterar a realidade no sentido da justiça**: uma sociedade mais justa é mais pacífica e próspera (atuação na causa e não nos efeitos).

Conclusões gerais

- A tecnologia está, portanto, ao serviço de uma **conceção positivista-utilitarista do mundo**: tendo por objetivo a tomada de decisões favoráveis (para quem as toma) numa **lógica custo-benefício** (economicismo); o que interessa é prever a realidade futura, para que se possam calcular os custos e os benefícios;
    - O positivismo procura reduzir a realidade à análise dos fenómenos realizados; visão muito útil e adequada à realidade tecnológica e tão pouco científica.
    - Numa perspetiva utilitarista, importa aferir as decisões que produzem mais benefícios, numa lógica de custo-benefício.
- Se não se tiver em conta que o direito visa alterar a realidade no sentido da justiça, o **direito ou permite esta conceção** (por exemplo pela utilização pelos tribunais de software como o COMPAS: maximiza-se o benefício para a sociedade, com menor custo) **ou até estimula** a (sobrevalorização da segurança jurídica);
- O maior perigo é então que o direito se desvirtue e seja instrumentalizado, e que a sociedade se torne mais injusta;
- Determinar o justo é uma atividade inerentemente artesanal, casuística e humana, pelo que não é possível recorrer a esta lógica.