UE VENCE CORRIDA DA REGULAÇÃO DA IA

Após longas negociações sobre a vigilância biométrica e os sistemas como o ChatGPT, a UE tornou-se finalmente a primeira potência mundial a estabelecer regras claras para a IA. Mas os receios sobre o entrave à inovação mantêm-se.

RITA SOUSA E SILVA

É OFICIAL: a União Europeia (UE) é pioneira na elaboração de uma regulação concreta para a Inteligência Artificial (IA). Após uma ronda de negociações de 38 horas, os legisladores europeus chegaram a um acordo provisório, no dia 8 de dezembro, sobre as regras que irão reger a utilização destas tecnologias.

A obtenção de acordo não foi um mar de rosas, sendo marcada por um atraso significativo devido sobretudo a "dois pontos mais problemáticos": "a proibição da utilização de sistemas biométricos de identificação remota de pessoas pelas autoridades públicas; e a inexistência de regras para sistemas genéricos de IA (como o ChatGPT)", explica Daniel Reis, Sócio de IPT da DLA Piper.

O debate sobre o *Artificial Intelligence Act* (AI Act) foi igualmente assinalado por uma onda de receios sobre a possibilidade da criação de uma regulação rígida que travasse a inovação, a evolução tecnológica e a competitividade no espaço europeu.

CHATGPT COMO FORÇA DISRUPTIVA

As regras do AI Act seguem uma abordagem baseada no risco. O texto legislativo proíbe a utilização e colocação no mercado dos sistemas de IA classificados como sendo de risco inaceitável, como manipulação cognitivo-comportamental, eliminação não direcionada de imagens faciais da Internet ou imagens de CCTV, pontuação social e sistemas de categorização biométrica para inferir crenças políticas, religiosas, filosóficas, orientação sexual e raça. Ademais, são impostos requisitos mínimos de transparência para os sistemas de IA de risco limitado e obrigações mais exigentes para os de elevado risco, como é o caso do ChatGPT.

"O que deu uma complicação maior na discussão do AI Act foi a entrada no mercado dos sistemas como o ChatGPT, porque demonstrou como a tecnologia de alto impacto trouxe riscos muito evidentes – riscos a direitos de autor, riscos à privacidade – e isso não estava ainda bem endereçado no texto", aponta Eduardo Magrani, Consultor Sénior de TMT da CCA Law Firm.

Relativamente a estes sistemas, "houve agora consenso que deveriam ser colocados no mercado com maior transparência", nomeadamente "dos desenvolvedores, pedindo para informar a base de dados que foi usada para treinar a IA e, eventualmente, dependendo do risco, podem ter de pedir autorização", explica o advogado. Além disto, deverão publicar "documentação técnica dos dados para treinamento e se existem proteções a direitos de autor", bem como informar os

- Eduardo Magrani, CCA Law Firm -

"próprios indivíduos de que aquele conteúdo está a ser produzido por generative AI".

Por outro lado, "uma regulação baseada em riscos gastou muito tempo a tentar perceber que tecnologias deveriam entrar em cada categoria". Um exemplo são as "tecnologias *deepfake*, [que] não estavam como alto risco; estavam com um risco ainda muito baixo. Isto são tecnologias que podem ser usadas até para manipulação democrática".

VIGILÂNCIA BIOMÉTRICA E DIREITOS HUMANOS

A questão da vigilância biométrica foi um ponto difícil no processo de negociações, uma vez que "traz o choque entre os princípios importantes na ordem democrática – de um lado, o princípio da privacidade e, de outro, o princípio da segurança pública e da segurança nacional", considera Eduardo Magrani.

Neste sentido, a tecnologia "pode afetar direitos humanos pela desproporcionalidade da sua aplicação", reforça o advogado. Por exemplo, "se o reconhecimento biométrico facial for utilizado em vias públicas de forma indiscriminada, a privaci-

- Daniel Reis, DLA Piper -

dade dos indivíduos pode estar a ser afetada de forma desproporcional".

"O anexo que identifica as aplicações proibidas incluía a vigilância biométrica remota por autoridades públicas", refere Daniel Reis. "Este ponto era defendido pelo Parlamento, sendo que alguns Estados-Membros (incluindo Alemanha, França e Itália) defendiam que esta aplicação deveria ser considerada de alto risco (ou seja, permitida em determinadas circunstâncias), e não proibida. Foi a posição destes Estados-Membros que prevaleceu".

Desta forma, os legisladores europeus acordaram que os governos só poderão utilizar a vigilância biométrica em tempo real em espaços públicos em casos de vítimas de determinados crimes, na prevenção de ameaças genuínas, presentes ou previsíveis, como ataques terroristas, e na busca de pessoas suspeitas de crimes mais graves.

INOVAÇÃO VS. REGULAÇÃO

Uma das principais críticas ao AI Act é o entrave à inovação e à competitividade. As maiores empresas europeias – como a Siemens, Heineken, Renault e Airbus – manifestaram-se contra a proposta aprovada pelo Parlamento Europeu em junho, considerando que "comprometeria a competitividade e a soberania tecnológica da Europa". Também os Estados Unidos alertaram que esta prejudicaria as pequenas empresas e beneficiaria apenas as grandes organizações capazes de cobrir os custos de *compliance*.

Segundo Daniel Reis, importa distinguir "o impacto do AI Act para os produtores de IA do impacto para os utilizadores de IA". No que diz respeito aos produtores, "o impacto é muito significativo, ao impor um catálogo alargado de obrigações a estas empresas". Existe ainda um "efeito extraterritorial" do diploma: "estas regras também afetam produtores estabelecidos fora da UE que queiram vender dentro da UE".

"Já para os utilizadores, o AI Act vem trazer segurança e clareza, e promoverá a adoção de soluções de IA", considera o advogado. "Na minha opinião, não obstante o 'pé pesado' da UE, a entrada em vigor do AI Act irá beneficiar o mercado e as empresas".

Para Eduardo Magrani, "é possível ter uma regulação que favoreça a inovação". "A mitigação de riscos não chega a eliminar a inovação; pelo contrário, pode permitir inovações, mas responsáveis", frisa. "Pode permitir que a competição no mercado seja dada em bases de produção de desenvolvimento de maior qualidade".

A LEBRE E A TARTARUGA

Aprovado o texto legislativo, alguns críticos acreditam que o AI Act relembra a história da tartaruga e a lebre. Visando tornar-se pioneira na regulação da IA, a UE poderá ter-se apressado no estabelecimento de regras sem saber exatamente aquelas que poderão ser necessárias.

"É por isso que a aprovação tem demorado a acontecer", aponta Eduardo Magrani. A entrada no mercado do ChatGPT foi um exemplo notório. "Os reguladores viram que [o texto] não estava preparado para regular a tecnologia – isto pode tornar a acontecer, não é?", pondera o advogado.

"O desenvolvimento tecnológico não vai frear com aprovação do AI Act e é por isso que é preciso ter uma regulação que consiga acompanhar esse desenvolvimento tecnológico", reforça. "Para isso, são muito importantes princípios como a transparência, como a utilização de medidas mitigadoras de risco".

Será no processo de implementação da regulação que se tornarão evidentes as suas potenciais lacunas. "A categorização dos riscos é ainda um tema que pode envolver lacunas muito sérias", considera Eduardo Magrani. "Vamos aprender quais são exatamente os *gaps* do AI Act na hora em que uma tecnologia como um *deepfake* causar um impacto enorme; por exemplo, se deveria de facto entrar numa área de alto risco ou numa alguma categoria diferente".

Além disto, "ainda que seja uma lei robusta, a implementação dela ainda não está tão clara", defende o advogado, considerando que não existe "clareza ainda sobre a criação das autoridades em cada país que vão ficar responsáveis por isso; então, preocupo-me com *enforcement* do AI Act".

Prevê-se que a Lei da IA entrará em vigor no final de 2025 ou no início de 2026. "O acordo alcançado é provisório. Falta vermos o texto consolidado, e ainda a aprovação definitiva. No processo legislativo europeu muitas vezes os detalhes são importantes, teremos de aguardar", afirma Daniel Reis. "E não podemos esquecer o Regulamento ePrivacy, tantas vezes anunciado e nunca concretizado: antes da publicação é sempre cedo cantar vitória". ■