RISK

CIBERCRIME E DIREITOS HUMANOS: OS PERIGOS DO TRATADO DA ONU

POR RITA SOUSA E SILVA

O TRATADO DA ONU SOBRE CIBERCRIME VISA PROPORCIONAR A COOPERAÇÃO INTERNACIONAL NA INVESTIGAÇÃO DE CASOS CRIMINAIS E OBTENÇÃO DE PROVA DIGITAL. MAS ATÉ QUE PONTO É QUE A CONVENÇÃO DEIXARÁ CAIR OS DIREITOS HUMANOS E SE TORNARÁ NUM INSTRUMENTO DE VIGILÂNCIA ESTATAL?

Com a dimensão global do cibercrime, torna-se difícil investigar casos criminais no ciberespaço sem uma cooperação internacional que permita às autoridades aplicar a lei no estrangeiro. É neste contexto que nasceu a necessidade de criar uma convenção global sobre cibercrime, elaborada pela ONU e ratificada pelos 193 estados-membros. Com visões cada vez mais polarizadas, organizações e empresas receiam que o texto trará mais perigos do que benefícios.

Não é a primeira vez que é concebido um instrumento jurídico global contra o cibercrime. Em 2001, a Convenção de Budapeste, a primeira internacional sobre a matéria, foi assinada por 64 países, contando hoje com 68, e entrou em vigor em 2004.

Países como a China, a Rússia, a Índia e o Brasil recusaram juntar-se, muito devido à "exigência de respeito dos direitos humanos" estipulada no documento, refere Pedro Verdelho, diretor do Gabinete de Cibercrime da Procuradoria-Geral da República e representante de Portugal no Comité da Convenção de Budapeste.

Reconhecendo a importância da colaboração transnacional, a Rússia, com o apoio posterior da China, propôs a criação de uma nova convenção sobre o cibercrime na Assembleia Geral das Nações Unidas – uma resolução aprovada pela ONU em maio de 2021. O projeto de tratado deverá ser aprovado em Assembleia até setembro de 2024.

Os trabalhos do comité *ad hoc* são abertos à sociedade civil, contando com a participação de ONG, universidades e empresas, que puderam candidatar-se ao estatuto de *stakeholders* em 2021, para assistir e participar ativamente nas sessões. O Center for Cooperation in Cyberspace (CCC) é a única ONG portuguesa a participar na convenção.

Terminada a penúltima ronda de negociações no início de setembro, o consenso parece estar cada vez mais longínquo. "As visões são tão díspares que nós

corremos o sério risco, hoje, de vir a não ter convenção", revela Filipe Domingues, co-fundador do CCC. "*Acaba por ser um reflexo perfeito da fragmentação geopolítica a que estamos a assistir*".

As divergências entre os estados-membros, influenciadas em parte pelos seus modelos de governação, resumem-se a duas visões: por um lado, os países do Ocidente, que defendem a "introdução de cláusulas estritas de respeito pelos direitos fundamentais, expressando aqui fortes exigências", explica Pedro Verdelho; por outro, Rússia, Irão, Egipto, Cuba, Venezuela, e outros Estados, que "mostraram maior resistência e desejo de limitar várias destas disposições".

O QUE É O CIBERCRIME?

Dois anos e seis rondas de negociação passadas, a definição do próprio conceito de cibercrime e do âmbito do tratado continuam em cima da mesa. "A dificuldade não é aparente, é real", reconhece Daniel Reis, advogado da DLA Piper. "O que está em causa é criar a primeira definição legal sobre o cibercrime".

PEDRO VERDELHO, PROCURADORIA-GERAL DA REPÚBLICA

Ainda não está acordada a lista de ações criminalizadas, estando a ser discutido a inclusão de crimes *cyber enabled* (ciberpotenciados) ou exclusivamente de *cyber dependent* (ciberdependentes), constata Filipe Domingues.

A posição é consensual no Ocidente e entre países com visões semelhantes, como o Japão, a Austrália e a Nova Zelândia, considerando que o tratado da ONU deverá incidir apenas sobre os crimes *cyber dependent*, que remetem para "aqueles crimes que precisam de

NA CONVENÇÃO DE 2001, PAÍSES COMO A CHINA, A RÚSSIA, A ÍNDIA E O BRASIL RECUSARAM JUNTAR-SE, MUITO DEVIDO À "EXIGÊNCIA DE RESPEITO DOS DIREITOS HUMANOS".

PEDRO VERDELHO, DIRETOR DO GABINETE DE CIBERCRIME DA PROCURADORIA-GERAL DA REPÚBLICA

FILIPE DOMINGUES, CO-FUNDADOR DO CCC

uma rede de computadores ou de um computador para serem cometidos", explica o co-fundador do CCC.

Porém, para outros países, o âmbito da convenção deve abranger os *cyber enabled*, ou seja, "um conjunto de ilegalidades que não dependem de tecnologias informáticas para serem cometidos, mas que podem ser potenciados por essas tecnologias".

VISÕES EM CHOQUE

"Tanto do lado ocidental como do lado não ocidental têm surgido propostas que são simplesmente inaceitáveis para os dois lados", indica Filipe Domingues.

Estados como o Vietname querem remover totalmente a linguagem de direitos humanos, enquanto o Uruguai e a Austrália visam reforçá-la. A China e outros países, por sua vez, tentaram limitar as secções sobre os direitos humanos a países que ratificaram tratados separados, como o Pacto Internacional sobre Direitos Civis e Políticos (PIDCP).

> "AS VISÕES SÃO TÃO DÍSPARES QUE NÓS CORREMOS O SÉRIO RISCO, HOJE, DE VIR A NÃO TER CONVENÇÃO"
>
> FILIPE DOMINGUES, CO-FUNDADOR DO CCC

Em janeiro, durante as negociações em Viena, a delegação chinesa propôs uma redefinição do conceito de cibercrime para incluir a divulgação de *fake news* online, enquanto diplomatas do Paquistão e do Irão procuraram introduzir uma secção que estabeleceria os insultos religiosos como um cibercrime.

"A criminalização de comportamentos como as *fake news* ou insultos religiosos pode atentar gravemente contra a liberdade de expressão, limitando a liberdade de opinião, por exemplo, nas redes sociais", alerta Francisco Pimenta, advogado da CCA Law Firm.

Muitas destas propostas foram deixadas cair pelo grupo de trabalho ao longo das sessões, não reunindo um "consenso mínimo". Pedro Verdelho expõe que, no entanto, "algumas delegações, com destaque para a da Federação Russa, insistiram em propostas suas anteriores – mesmo sabendo que a maioria

> "O QUE ESTÁ EM CAUSA É CRIAR A PRIMEIRA DEFINIÇÃO LEGAL SOBRE O CIBERCRIME".
>
> DANIEL REIS, ADVOGADO DA DLA PIPER

dos Estados não as subscreve. Esta abordagem gerou uma atmosfera geral de inflexibilidade".

DIREITOS HUMANOS EM PERIGO

O projeto de tratado tem sido alvo de fortes críticas, particularmente pela parte de várias organizações de direitos humanos. Durante as negociações mais recentes, as preocupações cresceram de tal forma que várias ONG organizaram uma conferência de imprensa para discutir os perigos do texto, receando a expansão do poder de vigilância dos governos e o fornecimento de ferramentas de repressão às ditaduras.

Entre as várias disposições contestadas, o Artigo 23.º é referido frequentemente por trazer "consigo a possibilidade de aumentar a vigilância sobre os cidadãos de uma forma preocupante", identificando a "necessidade de assegurar a recolha de prova digital relacionada com qualquer tipo de crime, independentemente da sua gravidade ou do crime estar associado a um sistema informático", adverte Jorge Pinto, presidente da Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI).

Ademais, no seu estado atual, a convenção permite aos governos "o acesso em tempo real, de dados de tráfego e comunicações, sem necessidade de prévia autorização judicial", mesmo em investigações de "crimes que nem sequer assumem natureza informática pura" e "desde que para fins de recolha de prova de natureza informática/eletrónica", analisa

DANIEL REIS, ADVOGADO DA DLA PIPER

Francisco Pimenta. Para o advogado, isto "permite um exercício de poder de vigilância dos estados com um espectro tão alargado que quase resulta num autoritarismo informático".

Uma proposta controversa apresentada foi a realização de investigações criminais em total sigilo, sem notificar os alvos de vigilância que os seus dados estão a ser acedidos. Em contraste, na penúltima sessão de negociações, a Comissão Europeia "seguramente consciente do que estava

FRANCISCO PIMENTA, CCA LAW FIRM

a fazer, fez uma proposta tão radical na proteção dos dados pessoais, que, se fosse tornada lei, impediria qualquer investigação criminal", relata Filipe Domingues.

A proposta determinava que, cada vez que um país solicitasse um pedido de preservação de dados, "haveria uma *due diligence* para garantir que o pedido estava de acordo com toda a legislação em matéria de direitos humanos, de proteção da privacidade". Com o tempo que demoraria, "o período habitual de preservação dos dados expiraria e, quando estivesse terminada a *due diligence*, já não haveria dados para investigar", completa.

Para além disto, a falta de controlo na colaboração transfronteiriça entre governos poderá afetar a proteção de dados pessoais e a privacidade dos cidadãos em vários níveis, colocando em causa os padrões de proteção de dados existentes no mundo. "É bastante claro que o texto atual não tem salvaguardas suficientes para proteger os cidadãos de cada país contra uma utilização indevida dos seus dados pessoais", defende Jorge Pinto.

Para o presidente da AP2SI, o texto atual "abre a possibilidade de abuso por parte de Estados com poucos controlos ou verificações", como, por exemplo, "a recolha de informação sobre dissidentes ou ativistas políticos que estejam localizados noutros países".

INVESTIGAÇÃO E EMPRESAS TECNOLÓGICAS

A ameaça ao trabalho dos investigadores de cibersegurança e dos hackers éticos é outra preocupação sentida por várias organizações e empre-

> "A CRIMINALIZAÇÃO DE COMPORTAMENTOS COMO AS FAKE NEWS OU INSULTOS RELIGIOSOS PODE ATENTAR GRAVEMENTE CONTRA A LIBERDADE DE EXPRESSÃO, LIMITANDO A LIBERDADE DE OPINIÃO, POR EXEMPLO, NAS REDES SOCIAIS",
>
> FRANCISCO PIMENTA, ADVOGADO DA CCA LAW FIRM

sas, devido às restrições impostas na investigação de vulnerabilidades.

Está em vias de discussão "a necessidade de o recurso pelos governos às ferramentas de investigação resultantes da Convenção ser sempre precedido de autorização judicial prévia", esclarece Francisco Pimenta, sendo o pedido instruído "como uma descrição e fundamentação do razão da necessidade de acesso aos dados solicitados".

JORGE PINTO, AP2SI

> O ARTIGO 23.º É REFERIDO FREQUENTEMENTE POR TRAZER "CONSIGO A POSSIBILIDADE DE AUMENTAR A VIGILÂNCIA SOBRE OS CIDADÃOS DE UMA FORMA PREOCUPANTE", IDENTIFICANDO A "NECESSIDADE DE ASSEGURAR A RECOLHA DE PROVA DIGITAL RELACIONADA COM QUALQUER TIPO DE CRIME, INDEPENDENTEMENTE DA SUA GRAVIDADE OU DO CRIME ESTAR ASSOCIADO A UM SISTEMA INFORMÁTICO".
>
> JORGE PINTO, PRESIDENTE DA ASSOCIAÇÃO PORTUGUESA PARA A PROMOÇÃO DA SEGURANÇA DA INFORMAÇÃO (AP2SI).

A autorização legal em questão seria concedida mediante "um juízo de proporcionalidade entre a necessidade de intrusão nos direitos de privacidade dos indivíduos e a essencialidade para a investigação", acrescenta.

Ainda mais, Francisco Pimenta explica que as empresas tecnológicas poderiam ver a sua atividade a ser "livremente controlada nestes termos" e, devido à sua base informática, "bloqueada por parte das entidades inspetivas de cada um dos estados-membros" ou até estrangeiras, graças à "livre partilha de dados obtidos no âmbito destas investigações".

Para o advogado, isto poderá conduzir a um "estado de quase autoritarismo digital, com um controlo de informação e dados imediato, constante e livre de quaisquer ónus".

A Microsoft foi a primeira grande empresa de tecnologia a manifestar-se contra a convenção da ONU. No final de agosto, Amy Hogan-Burney, uma representante do departamento de política de cibersegurança da empresa, recorreu ao Linkedin para tecer duras críticas ao projeto de tratado, considerando-o demasiado amplo e aberto a interpretação.

Na sua publicação do Linkedin, Hogan-Burney afirma que "os hackers éticos que trabalham para identificar vulnerabilidades, simular ciberataques e testar as defesas do sistema precisam de ser protegidos" e muitas disposições "não incluem uma referência à 'intenção criminosa', o que garantiria que atividades como testes de penetração permanecessem legais".

FUTURO DA CONVENÇÃO É INCERTO

As profundas divisões entre os estados-membros aparentam não ser conciliáveis na matéria de direitos humanos e vigilância governamental. "Ainda existem divergências fortes, que terão inevitavelmente de ser debatidas e resolvidas", prevê Pedro Verdelho. "Seria preferível aprovar o projeto da futura Convenção por consenso. Mas, quanto a alguns aspetos, a votação parece inevitável, para evitar o colapso do processo. A votação conduzirá a dificuldades na aceitação e ratificação subsequente pelos Estados-Membros".

Filipe Domingues revela que o processo está "muito atrasado". Na sexta ronda de negociações, a presidente do comité acrescentou nove horas extra de reuniões. A sétima e última, que ocorrerá entre janeiro e fevereiro de 2024, deveria servir somente para "coroar ou matar o tratado". No entanto, adianta que "não vai ser assim, porque o texto está todo vermelho, cheio de *track changes*".

Face à dificuldade em chegar a consenso, a solução poderá passar pela criação de um tratado com condições mínimas: "as indicações que nós temos é de que ainda não caiu totalmente a hipótese de ter uma convenção minimalista, baseada em denominadores comuns mínimos, à qual poderá ser mais tarde, seja daqui a dez anos, seja daqui a 20, acrescentado um protocolo adicional", revela o co-fundador do CCC.

O futuro da convenção da ONU sobre cibercrime não é certo e o seu sucesso poderá estar em risco. "Se nós, por um lado, estamos otimistas em relação à capacidade que os estados ocidentais têm de proteger os nossos direitos humanos e as nossas liberdades e garantias, não estamos tão otimistas em relação a um desfecho positivo deste tratado", confessa Filipe Domingues. "Continua a haver atores estatais e não estatais que não tem problema rigorosamente nenhum em deitar este processo abaixo, desde que isso impeça a agenda de estados como a Rússia e a China". ◀