Parlamento Europeu
2014-2019

Documento de sessão

A8-0044/2017

20.2.2017

RELATÓRIO

sobre as implicações dos grandes volumes de dados nos direitos fundamentais: privacidade, proteção de dados, não discriminação, segurança e aplicação da lei (2016/2225(INI))

Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

Relatora: Ana Gomes

ÍNDICE

Página

PROPOSTA DE RESOLUÇÃO DO PARLAMENTO EUROPEU

sobre as implicações dos grandes volumes de dados nos direitos fundamentais: privacidade, proteção de dados, não discriminação, segurança e aplicação da lei (2016/2225(INI))

O Parlamento Europeu,

– Tendo em conta o artigo 16.º do Tratado sobre o Funcionamento da União Europeia,

– Tendo em conta os artigos 1.º, 7.º, 8.°, 11.°, 14.º, 21.°, 47.º e 52.º da Carta dos Direitos Fundamentais da União Europeia,

– Tendo em conta as Diretrizes para a regulamentação dos ficheiros informatizados de dados pessoais, emitidas pela Assembleia-Geral das Nações Unidas na sua Resolução 45/95 de 14 de dezembro de 1990,

– Tendo em conta o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento geral sobre a proteção de dados)[1], bem como a Diretiva 2016/680 do Parlamento Europeu e do Conselho, de 27 da abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho[2],

– Tendo em conta a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, de 6 de maio de 2015, intitulada «Estratégia para o Mercado Único Digital na Europa» (COM(2015) 0192),

– Tendo em conta a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de janeiro de 1981 (STE 108), e o seu Protocolo Adicional, de 8 de janeiro de 2001 (STE 181)[3],

– Tendo em conta a Recomendação CM/Rec(2010)13 do Comité de Ministros do Conselho da Europa, de 23 de novembro de 2010, dirigida aos Estados-Membros sobre a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal no âmbito da definição de perfis[4],

– Tendo em conta o Parecer 7/2015 da Autoridade Europeia para a proteção de dados, de 19 de novembro de 2015, intitulada «Meeting the challenges of big data; A call for transparency, user control, data protection by design and accountability» (Enfrentar os desafios dos grandes volumes de dados: um convite para a transparência, o controlo por

[1] JO L 119 de 4.5.2016, p. 1
[2] JO L 119 de 4.5.2016, p. 89
[3] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
[4] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00

parte dos utilizadores, a proteção de dados desde a conceção e a responsabilidade)[1],

– Tendo em conta o parecer 8/2016 da Autoridade Europeia para a Proteção de Dados, de 23 de setembro de 2016, intitulado «Parecer da AEPD sobre a aplicação coerente dos direitos fundamentais na era dos grandes volumes de dados»[2],

– Tendo em conta a declaração do Grupo de Trabalho do artigo 29.º, de 16 de setembro de 2014, sobre o impacto do desenvolvimento de grandes volumes de dados sobre a proteção das pessoas relativamente ao tratamento dos seus dados pessoais na UE[3],

– Tendo em conta o artigo 52.º do seu Regimento,

– Tendo em conta o relatório da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (A8-0044/2017),

A. Considerando que o termo «grandes volumes de dados» se refere à recolha, análise e acumulação recorrente de grandes quantidades de dados, incluindo dados pessoais, a partir de diversas fontes, que são objeto de um tratamento automatizado por algoritmos informáticos e técnicas avançadas de tratamento de dados, utilizando tanto dados armazenados como dados transmitidos em fluxo, a fim de identificar determinadas correlações, tendências e padrões (análise de grandes volumes de dados);

B. Considerando que certos casos de utilização de grandes volumes de dados incluem também a preparação de dispositivos de inteligência artificial, como as redes neuronais e os modelos estatísticos, a fim de prever determinados acontecimentos e comportamentos; que os dados de preparação são, muitas vezes, de qualidade duvidosa e não neutros;

C. Considerando que a evolução das tecnologias da comunicação e a utilização generalizada de dispositivos eletrónicos, de gadgets de monitorização, de redes sociais e as interações e redes na Internet, incluindo dispositivos que comunicam informações sem intervenção humana, levaram ao desenvolvimento de enormes conjuntos de dados, em constante crescimento, que, através de análise e de técnicas avançadas de tratamento, fornecem informações sem precedentes sobre o comportamento humano, a vida privada e as nossas sociedades;

D. Considerando que os serviços de informações dos países terceiros e dos Estados-Membros têm recorrido cada vez mais ao tratamento e à análise de tais conjuntos de dados, os quais ou não estão cobertos por qualquer quadro jurídico ou, mais recentemente, foram objeto de legislação cuja compatibilidade com o direito primário e secundário da UE é motivo de preocupação e continua por determinar;

E. Considerando que o aumento da intimidação, da violência contra as mulheres e da vulnerabilidade das crianças se verifica também no ambiente em linha; que a Comissão

[1] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf
[2] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-23_BigData_opinion_EN.pdf
[3] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

e os Estados-Membros devem adotar todas as medidas jurídicas necessárias para combater estes fenómenos;

F. Considerando que cada vez mais sociedades, empresas, organismos e agências, organizações governamentais e não governamentais (bem como os setores público e privado em geral), líderes políticos, a sociedade civil, a comunidade académica e científica e os cidadãos em geral tiram partido desses conjuntos de dados e da análise de grandes volumes de dados para estimular a competitividade, a inovação, a previsão dos mercados, as campanhas políticas, a publicidade direcionada, a investigação científica e a elaboração de políticas no domínio dos transportes, da fiscalidade, dos serviços financeiros, das «cidades inteligentes», da aplicação da lei, da transparência, da saúde pública e da resposta a catástrofes, e para influenciar as eleições e os resultados políticos através, nomeadamente, de comunicações específicas;

G. Considerando que o mercado dos grandes volumes de dados está a crescer à medida que a tecnologia e o processo decisório baseado em dados são cada vez mais reconhecidos como fornecedores de soluções; que ainda não existe uma metodologia para efetuar uma avaliação, com base em dados concretos, do impacto total dos grandes volumes de dados, mas que há indicações de que a análise dos grandes volumes de dados é suscetível de ter um impacto horizontal significativo, tanto no setor público, como privado; que a Estratégia da Comissão para o Mercado Único Digital na Europa reconhece o potencial das tecnologias e dos serviços baseados em dados e dos grandes volumes de dados para atuarem como catalisadores do crescimento económico, da inovação e da digitalização na UE;

H. Considerando que a análise dos grandes volumes de dados cria valor acrescentado por várias vias e que há uma série de exemplos positivos que oferecem oportunidades significativas aos cidadãos, por exemplo, nos domínios dos cuidados de saúde, da luta contra as alterações climáticas, da redução do consumo energético, da melhoria da segurança dos transportes e da possibilidade de criação de «cidades inteligentes», aumentando, assim, a otimização e a eficiência das empresas e contribuindo para melhorar as condições de trabalho e detetar e combater a fraude; que os grandes volumes de dados proporcionam vantagens competitivas para os processos de tomada de decisão das empresas europeias, enquanto o setor público pode beneficiar de uma maior eficiência graças a informações mais exatas sobre os diferentes níveis de desenvolvimento socioeconómico;

I. Considerando que os grandes volumes de dados oferecem os potenciais acima mencionados aos cidadãos, à comunidade académica e científica e aos setores público e privado, mas também implicam riscos significativos, nomeadamente no que diz respeito à proteção dos direitos fundamentais, como o direito à privacidade e à proteção e segurança dos dados, bem como a liberdade de expressão e a não discriminação, tal como garantidos pela Carta dos Direitos Fundamentais da UE e pelo direito da União; que as técnicas de pseudonimização e cifragem podem atenuar os riscos relacionados com a análise de grandes volumes de dados e, por isso, desempenham um papel importante na salvaguarda da privacidade do titular, ao mesmo tempo que promovem a inovação e o crescimento económico; que estes elementos devem ser considerados como parte da revisão em curso da Diretiva relativa à privacidade;

J. Considerando que a presença generalizada de sensores, a larga produção de dados de rotina e as atuais atividades de tratamento de dados nem sempre são suficientemente transparentes, dificultando a capacidade dos cidadãos e das autoridades para avaliarem os processos e a finalidade da recolha, compilação, análise e utilização de dados pessoais; que se observa uma diluição dos dados pessoais e não pessoais decorrente da análise dos grandes volumes de dados, que é suscetível de criar novos dados pessoais;

K. Considerando que o setor dos grandes volumes de dados está a crescer a um ritmo de 40 % ao ano, ou seja sete vezes mais rapidamente do que o mercado de TI; que a concentração de grandes conjuntos de dados produzidos pelas novas tecnologias oferece informações cruciais para grandes sociedades, o que implica mudanças sem precedentes no equilíbrio de poderes entre cidadãos, governos e intervenientes privados; que a concentração do poder nas mãos das sociedades poderia consolidar os monopólios e as práticas abusivas e ter um efeito nocivo nos direitos dos consumidores e na concorrência leal no mercado; que cumpre reforçar o controlo das concentrações de grandes volumes de dados pelo prisma dos interesses das pessoas individuais e da proteção dos direitos fundamentais;

L. Considerando que os grandes volumes de dados têm um enorme potencial inexplorado enquanto motor da produtividade e como forma de proporcionar melhores produtos e serviços aos cidadãos; sublinha, no entanto, que a utilização generalizada de dispositivos inteligentes, redes e aplicações Web por cidadãos, empresas e organizações não é necessariamente uma prova da satisfação relativamente à oferta de produtos, mas sim um reconhecimento geral do facto de estes serviços se terem tornado indispensáveis para viver, comunicar e trabalhar, apesar da falta de compreensão dos riscos que possam implicar para os nossos direitos, segurança e bem-estar;

M. Considerando que é necessário distinguir a quantidade de dados da qualidade dos dados, a fim de permitir uma utilização eficaz dos grandes volumes de dados (algoritmos e outros instrumentos analíticos); que os dados e /ou os procedimentos de baixa qualidade em que se baseiam os processos de tomada de decisão e os instrumentos analíticos podem traduzir-se em algoritmos parciais, correlações ilegítimas, erros, numa subestimação das implicações jurídicas, sociais e éticas, no risco de utilização de dados para fins discriminatórios ou fraudulentos e na marginalização do papel dos seres humanos nestes processos, podendo resultar em processos imperfeitos de tomada de decisão, com um impacto nocivo nas vidas e nas oportunidades dos cidadãos, mormente nos grupos marginalizados, bem como em consequências negativas para as sociedades e as empresas;

N. Considerando que a responsabilidade relativa aos algoritmos e a transparência devem implicar a aplicação de medidas técnicas e operacionais que garantam a transparência, a não discriminação dos processos de tomada de decisões automatizados e o cálculo de probabilidades de comportamento individual; que a transparência deve proporcionar aos cidadãos informações fiáveis sobre a lógica aplicada, o significado e as consequências previstas; que tal deve incluir informação sobre os dados utilizados para a formação em matéria de análise dos grandes volumes de dados e permitir às pessoas compreender e controlar as decisões que as afetam;

O. Considerando que a análise dos dados e os algoritmos têm um impacto cada vez maior

na informação disponibilizada aos cidadãos; que essas técnicas, quando usadas indevidamente, podem pôr em perigo os direitos fundamentais à informação, bem como a liberdade dos meios de comunicação social e o pluralismo; que a radiodifusão de serviço público nos Estados-Membros se encontra diretamente associada às necessidades de natureza democrática, social e cultural de cada sociedade, bem como à necessidade de preservar o pluralismo nos meios de comunicação social, tal como afirmado no Protocolo relativo ao serviço público de radiodifusão nos Estados-Membros, anexo ao Tratado de Amesterdão (11997D/PRO/09);

P. Considerando que a proliferação do tratamento e análise de dados, o número maciço de intervenientes envolvidos na recolha, conservação, tratamento, armazenamento e partilha de dados e a combinação de grandes conjuntos de dados que contêm dados pessoais e não pessoais de diversas fontes, embora ofereçam oportunidades significativas, criaram grandes incertezas para os cidadãos e para os setores público e privado sobre os requisitos específicos em matéria de cumprimento da legislação em vigor da UE em matéria de proteção de dados;

Q. Considerando que existem múltiplos sistemas tradicionais não estruturados, contendo grandes volumes de dados recolhidos por empresas durante muitos anos, com sistemas de governação de dados pouco claros, os quais devem ser sistematicamente repostos em conformidade;

R. Considerando que deve ser promovida uma maior cooperação e coerência entre as várias entidades reguladoras e as autoridades de supervisão da concorrência, da proteção dos consumidores e da proteção dos dados a nível nacional e da UE, a fim de garantir uma abordagem consistente e a compreensão das implicações dos grandes volumes de dados nos direitos fundamentais; que a criação e o desenvolvimento de uma câmara de compensação digital[1] enquanto rede voluntária dos organismos responsáveis pela aplicação da lei podem contribuir para melhorar o trabalho destes e as respetivas atividades de aplicação da lei, para além de ajudarem a reforçar as sinergias e a proteção dos direitos e interesses dos cidadãos;

Considerações gerais

1. Salienta que as perspetivas e as oportunidades oferecidas pelos grandes volumes de dados só podem ser plenamente aproveitadas pelos cidadãos, pelos setores público e privado e pela comunidade académica e científica quando a confiança do público nestas tecnologias for assegurada por uma aplicação rigorosa dos direitos fundamentais, pelo cumprimento da legislação em vigor da UE em matéria de proteção de dados e pela segurança jurídica para todas as partes envolvidas; salienta que o tratamento de dados pessoais só pode ser efetuado em conformidade com as bases jurídicas previstas no artigo 6.º do Regulamento (UE) n.º 2016/679; considera que a transparência e uma informação adequada do público visado são essenciais para reforçar a confiança do público e para a proteção dos direitos individuais;

2. Sublinha que o cumprimento da legislação existente em matéria de proteção de dados,

[1] Parecer 8/2016 da Autoridade Europeia para a Proteção de Dados, de 23 de setembro de 2016, intitulado «Parecer da AEPD sobre a aplicação coerente dos direitos fundamentais na era dos grandes volumes de dados», p. 15.

bem como a existência de normas científicas e éticas sólidas, são fundamentais para estabelecer um clima de confiança e a fiabilidade dos grandes volumes de dados; realça, além disso, que as informações reveladas pela análise de grandes volumes de dados não oferece um panorama imparcial de qualquer matéria e só são tão fiáveis quanto os dados subjacentes permitem; salienta que uma análise preditiva baseada em grandes volumes de dados apenas pode oferecer uma probabilidade estatística e, por conseguinte, nem sempre pode prever com exatidão o comportamento individual; salienta, por conseguinte, que normas científicas e éticas sólidas são vitais para a gestão da recolha de dados e para a avaliação dos resultados dessa análise;

3. Salienta que é possível inferir informações sensíveis sobre pessoas a partir de dados não sensíveis, o que torna ambígua a fronteira entre dados sensíveis e não sensíveis;

4. Salienta que a falta de conhecimento e compreensão dos cidadãos relativamente à natureza dos grandes volumes de dados possibilita a utilização não prevista das informações pessoais; assinala que a educação e a sensibilização sobre os direitos fundamentais são fundamentais na UE; insta as instituições da UE e os Estados-Membros a investirem na literacia digital e na sensibilização dos cidadãos, incluindo as crianças, para os direitos digitais, a privacidade e a proteção de dados; sublinha que tal formação deve incidir na compreensão dos princípios e da lógica do modo como funcionam os algoritmos e os processos decisórios automatizados, e como interpretá-los de forma significativa; salienta, além disso, a necessidade de educar com vista a promover o conhecimento sobre onde e como são recolhidos os fluxos de dados (recolha de material na Internet, combinação de fluxos de dados com dados das redes sociais e de dispositivos conectados, e respetiva concentração num novo fluxo);

Grandes volumes de dados para fins comerciais e no setor público

Privacidade e proteção de dados

5. Refere que a legislação da União relativa à proteção da vida privada e dos dados pessoais, o direito à igualdade e à não discriminação, bem como o direito das pessoas de receberem informações relativas à lógica subjacente aos processos de tomada de decisões e criação de perfis automatizados e o direito de recurso são aplicáveis ao tratamento de dados, quando esse tratamento for precedido de técnicas de pseudonimização ou, em todo o caso, quando a utilização de dados não pessoais possa ter um impacto sobre a vida privada das pessoas ou sobre outros direitos e liberdades, conduzindo à estigmatização de grupos inteiros da população;

6. Salienta que o mercado único digital deve assentar em redes e serviços de alta velocidade fiáveis e de confiança que salvaguardem os direitos fundamentais do titular à proteção dos dados e à privacidade, promovendo, ao mesmo tempo, a inovação e a análise de grandes volumes de dados, a fim de criar condições adequadas e uma concorrência equitativa para estimular a economia digital europeia;

7. Assinala, além disso, a possibilidade de re-identificação de pessoas através da conjugação dos diferentes tipos de dados anonimizados; salienta que a legislação da União relativa à proteção da vida privada e dos dados pessoais é aplicável ao tratamento desses dados correlacionados apenas quando uma pessoa é efetivamente re-identificável;

8. Insiste em que os princípios acima mencionados devem servir para enquadrar os processos de tomada de decisão dos setores público e privado e outros intervenientes que utilizem dados; salienta a necessidade de uma maior transparência e responsabilidade relativamente aos algoritmos no que se refere ao tratamento e à análise de dados por parte dos setores público e privado e outros intervenientes que recorram à análise de dados, enquanto instrumento essencial para garantir que os cidadãos são devidamente informados sobre o tratamento dos seus dados pessoais;

9. Destaca o papel fundamental que a Comissão, o Comité Europeu para a Proteção de Dados, as autoridades nacionais responsáveis pela proteção de dados e outras autoridades de supervisão independentes devem desempenhar no futuro, a fim de promover a transparência e o devido procedimento, a segurança jurídica em geral e, mais especificamente, normas concretas de proteção dos direitos fundamentais e garantias associadas à utilização do tratamento e análise de dados por parte dos setores público e privado; solicita uma colaboração mais estreita entre as autoridades reguladoras de comportamento no ambiente digital, a fim de reforçar as sinergias entre os quadros regulamentares para os consumidores e as autoridades da concorrência e da proteção de dados; solicita recursos financeiros e humanos adequados para tais autoridades; reconhece, além disso, a necessidade de criar uma câmara de compensação digital;

10. Salienta que a finalidade intrínseca dos grandes volumes de dados deveria ser a realização de correlações comparáveis recorrendo à menor quantidade possível de dados pessoais; sublinha, a este respeito, que a ciência, as empresas e as comunidades públicas devem centrar-se na investigação e inovação no domínio da anonimização;

11. Reconhece que a pseudonimização, anonimização ou codificação dos dados pessoais podem reduzir os riscos para os titulares de dados em questão quando os dados pessoais são utilizados por aplicações de grandes volumes de dados; chama ainda a atenção para as vantagens da pseudonimização prevista pelo RGPD enquanto salvaguarda adequada; recorda que a anonimização é um processo irreversível, através do qual os dados pessoais deixam de poder ser utilizados apenas para identificar ou destacar uma pessoa singular; considera que as obrigações contratuais devem assegurar que os dados anonimizados não serão re-identificados através do uso de correlações adicionais resultantes da combinação de diferentes fontes de dados; exorta os setores público e privado e outros intervenientes envolvidos na análise de grandes volumes de dados a reverem regularmente esses riscos tendo em conta as novas tecnologias e a documentarem a adequação das medidas adotadas; insta a Comissão, o Comité Europeu para a Proteção de Dados e outras autoridades de supervisão independentes a prepararem orientações sobre a anonimização adequada dos dados, a fim de evitar futuros abusos destas medidas e acompanhar as práticas;

12. Exorta os setores público e privado e os outros responsáveis pelo tratamento de dados a recorrerem aos instrumentos previstos no regulamento geral sobre a proteção de dados, como códigos de conduta e sistemas de certificação, a fim de procurar obter uma maior certeza sobre as suas obrigações específicas ao abrigo da legislação europeia e a garantir que as suas práticas e atividades estão em conformidade com as normas e salvaguardas jurídicas da UE;

13. Exorta a Comissão e os Estados-Membros a garantirem que as tecnologias baseadas em dados não discriminem ou limitem o acesso a um ambiente pluralista na comunicação social, e que promovam antes a liberdade e o pluralismo desses meios; salienta que a cooperação entre governos, instituições de ensino e organizações de comunicação social desempenhará um papel central em assegurar que a educação para os meios de comunicação digitais seja apoiada, a fim de capacitar os cidadãos e proteger os seus direitos à informação e à liberdade de expressão;

14. Considera que a publicação de dados pessoais pelas autoridades públicas por razões de interesse público, como a prevenção da corrupção, dos conflitos de interesse, da fraude fiscal e do branqueamento de capitais, é admissível numa sociedade democrática, desde que os dados sejam comunicados em condições estabelecidas por lei, que sejam garantidas as proteções adequadas e que a referida publicação seja necessária para o objetivo prosseguido e seja proporcional ao mesmo;

Segurança

15. Reconhece o valor acrescentado do desenvolvimento tecnológico, que contribuirá para melhorar a segurança; reconhece que alguns dos riscos mais prementes relacionados com as atividades de tratamento de dados, como as técnicas relativas aos grandes volumes de dados (mormente no contexto da Internet das coisas), que constituem um motivo de preocupação para os cidadãos, incluem as falhas de segurança dos dados, o acesso não autorizado aos dados e a vigilância ilegal; considera que o combate a este tipo de ameaças, sem violar os direitos fundamentais, exige uma verdadeira cooperação concertada entre os setores público e privado, as autoridades responsáveis pela aplicação da lei e as autoridades de supervisão independentes; sublinha, a este respeito, que deve ser conferida particular atenção à segurança dos sistemas de administração pública em linha, bem como às medidas jurídicas adicionais, tais como a responsabilidade pelo software;

16. Considera que a utilização da criptografia de ponta a ponta deverá igualmente ser incentivada e, se necessário, mandatada, em conformidade com o princípio da proteção de dados desde a conceção; recomenda que, para este efeito, todos os futuros quadros legislativos proíbam especificamente os prestadores de serviços de criptografia, os serviços de comunicações e todas as outras organizações (a todos os níveis da cadeia de aprovisionamento) de autorizar ou facilitar as «funções-alçapão» («backdoors»);

17. Salienta que o aumento da geração de dados e fluxos de dados significa uma maior vulnerabilidade e novos desafios no domínio da cibersegurança; solicita, neste contexto, a aplicação do princípio da «privacidade desde a conceção e por defeito», o uso de técnicas de anonimização, se necessário, e de técnicas de cifragem, bem como a realização obrigatória de avaliações de impacto sobre a vida privada; salienta que estas medidas devem ser aplicadas por todos os intervenientes envolvidos na análise dos grandes volumes de dados nos setores público e privado e por outros agentes que efetuam o tratamento de dados sensíveis, como advogados, jornalistas e pessoas que trabalham no setor da saúde, de modo a garantir que os grandes volumes de dados não aumentam a exposição a riscos de segurança da informação;

18. Recorda que, em conformidade com o disposto no artigo 15.º da Diretiva 2000/31/CE, os Estados-Membros não imporão aos prestadores, para o fornecimento dos serviços de

transporte, armazenagem temporária e armazenagem em servidor, uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar ativamente factos ou circunstâncias que indiciem ilicitudes; recorda, em particular, que o Tribunal de Justiça da União Europeia, nos acórdãos C-360/10 e C-70/10, rejeitou medidas de «vigilância ativa» da quase totalidade dos utilizadores dos serviços em causa (fornecedores de acesso à Internet num caso e uma rede social num outro caso) e precisou que é proibida toda e qualquer medida que imponha ao prestador de serviços de armazenagem uma vigilância geral;

Não discriminação

19 Salienta que, devido aos conjuntos de dados e sistemas de algoritmos utilizados nas avaliações e previsões nas várias fases do tratamento de dados, ao recrutar ou avaliar os indivíduos ou ao determinar os novos hábitos de consumo dos utilizadores de redes sociais, os grandes volumes de dados podem traduzir-se não apenas numa violação dos direitos fundamentais das pessoas, mas também num tratamento diferenciado e na discriminação indireta de grupos de pessoas com características similares, nomeadamente no que diz respeito à equidade e à igualdade de oportunidades de acesso à educação e ao emprego;

20. Solicita à Comissão, aos Estados-Membros e às autoridades responsáveis pela proteção de dados que identifiquem e adotem todas as medidas possíveis para minimizar a discriminação e a parcialidade dos algoritmos e para desenvolver um quadro ético comum sólido para o tratamento transparente de dados pessoais e a tomada automatizada de decisões, que possa orientar a utilização dos dados e a atual aplicação da legislação da UE;

21. Insta a Comissão, os Estados-Membros e as autoridades responsáveis pela proteção de dados a avaliarem especificamente a necessidade de transparência, não só dos algoritmos, mas também relativamente a eventuais distorções nos dados de preparação utilizados para fazer extrapolações com base em grandes volumes de dados;

22. Recomenda às empresas que realizem avaliações periódicas do caráter representativo dos conjuntos de dados, que verifiquem se estes são afetados por distorções e desenvolvam estratégias para as superar; salienta a necessidade de rever a exatidão e relevância das previsões baseadas na análise de dados, tendo presentes as preocupações relativas à ética e à equidade;

Grandes volumes de dados para fins científicos

23. Salienta que a análise de grandes volumes de dados pode ser benéfica para o desenvolvimento científico e para a investigação; considera que o desenvolvimento e a utilização da análise de grandes volumes de dados para fins científicos devem decorrer no respeito dos valores fundamentais consagrados na Carta dos Direitos Fundamentais e em conformidade com a legislação relativa à proteção de dados em vigor na UE;

24. Recorda que no âmbito do RGPD, o tratamento posterior de dados pessoais para fins estatísticos só pode gerar dados agregados que não possam voltar a ser aplicados a pessoas;

Grandes volumes de dados para efeitos de aplicação da lei

Privacidade e proteção de dados

25. Recorda a todos os responsáveis pela aplicação da lei que recorrem ao tratamento e análise de dados que a Diretiva (UE) 2016/680[1]: regula o tratamento de dados pessoais efetuado pelos Estados-Membros para fins de aplicação da lei; exige que a recolha e o tratamento de dados pessoais para fins de aplicação da lei devem ser sempre adequados e pertinentes e não devem ser excessivos relativamente à finalidade específica, explícita e legítima para a qual são tratados; dispõe que a finalidade e a necessidade da recolha destes dados devem ser claramente demonstradas; prevê a proibição de todas as decisões baseadas unicamente no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos jurídicos que prejudiquem o titular dos dados ou que o afetem significativamente, a menos que tal seja autorizado pelo direito da União ou pela legislação do Estado-Membro que rege o responsável pelo tratamento, e que prevê garantias adequadas para os direitos e liberdades do titular dos dados, pelo menos o direito de obter intervenção humana por parte dos responsáveis pelo tratamento; insta a Comissão, o Comité Europeu para a Proteção de Dados e outras autoridades de supervisão independentes a apresentarem orientações, recomendações e melhores práticas, a fim de especificar os critérios e as condições aplicáveis às decisões baseadas na definição de perfis e à utilização de grandes volumes de dados para fins de aplicação da lei;

26. Salienta a importância de cumprir os requisitos da Diretiva (UE) 2016/680 no que se refere à realização de avaliações de impacto prévias e auditorias que tenham em conta preocupações de ordem ética, a fim de avaliar o caráter inclusivo, a precisão e a qualidade dos dados e de garantir que as pessoas visadas pelas decisões e/ou os intervenientes que participam nos processos de tomada de decisão tenham a possibilidade de compreender e contestar a recolha ou a análise, os padrões e as correlações e evitar quaisquer efeitos prejudiciais para alguns grupos de pessoas;

27. Salienta que a confiança dos cidadãos nos serviços digitais pode ser seriamente afetada pelas atividades governamentais de vigilância em massa e pelo acesso não autorizado das autoridades policiais a dados comerciais e a outros dados pessoais;

28. Recorda que a legislação que permite às autoridades públicas acederem, de modo geral, aos conteúdos das comunicações eletrónicas deve ser considerada suscetível de comprometer a essência do direito fundamental ao respeito da vida privada, tal como garantido pelo artigo 7.º da Carta dos Direitos Fundamentais;

29. Sublinha a necessidade de introduzir orientações e sistemas nos concursos públicos para modelos, instrumentos e programas de tratamento de dados baseados em grandes volumes de dados para fins de aplicação da lei, a fim de garantir que o código subjacente possa ser, e seja, controlado pelas autoridades de aplicação da lei antes da

[1] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

aquisição final e possa ser verificado do ponto de vista da adequação, correção e segurança, tendo em mente que a transparência e a responsabilização são limitadas por software próprio; assinala que certos modelos de previsão policial são mais compatíveis com a proteção da privacidade do que outros, por exemplo, nos casos em que são feitas previsões probabilísticas sobre locais ou eventos e não sobre pessoas singulares;

Segurança

30. Sublinha a necessidade absoluta de proteger as bases de dados policiais de falhas de segurança e do acesso ilegal, tendo em conta que tal constitui um motivo de preocupação para os cidadãos; considera, por conseguinte, que o combate a este tipo de riscos exige uma cooperação eficaz e concertada entre as autoridades responsáveis pela aplicação da lei, o setor privado, os governos e as autoridades independentes de supervisão da proteção dos dados; insiste na necessidade de garantir uma segurança adequada dos dados pessoais, em conformidade com o Regulamento (UE) 2016/679 e com a Diretiva (UE) 2016/680, e de minimizar as vulnerabilidades através de arquiteturas de bases de dados seguras e descentralizadas;

Não discriminação

31. Alerta para o facto de que, tendo em conta o caráter intrusivo das decisões e medidas tomadas pelas autoridades responsáveis pela aplicação da lei - incluindo através do tratamento e da análise de dados - sobre a vida e os direitos dos cidadãos, é necessária extrema prudência para evitar a discriminação ilegal e evitar visar uma pessoa ou um grupo de pessoas definido por referência à raça, cor, ou origem étnica ou social, características genéticas, língua, religião ou crença, opiniões políticas ou outras, riqueza, nascimento, deficiência, idade, género, expressão de género, identidade de género, orientação sexual, estatuto de residente, saúde, pertença a uma minoria nacional, que é muitas vezes alvo de definição de perfis étnicos ou de um policiamento reforçado, bem como pessoas que possam ser definidas por características específicas;apela a uma formação adequada para os coletores de dados da primeira linha e utilizadores de informações obtidas a partir da análise de dados;

32. Exorta as autoridades responsáveis pela aplicação da lei dos Estados-Membros, que utilizam a análise de dados, a garantirem os mais elevados padrões de ética na análise dos dados e a assegurarem uma intervenção humana e a responsabilização ao longo das várias fases do processo de tomada de decisão, não só para avaliar a representatividade, a precisão e a qualidade dos dados, mas também para avaliar a adequação das decisões a tomar com base nessas informações;

°

° °

33. Encarrega o seu Presidente de transmitir a presente resolução ao Conselho e à Comissão.

RESULTADO DA VOTAÇÃO FINAL NA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO

Data de aprovação	9.2.2017
Resultado da votação final	+: 37 –: 1 0: 1
Deputados presentes no momento da votação final	Michał Boni, Caterina Chinnici, Agustín Díaz de Mera García Consuegra, Tanja Fajon, Kinga Gál, Ana Gomes, Nathalie Griesbeck, Sylvie Guillaume, Monika Hohlmeier, Eva Joly, Dietmar Köster, Barbara Kudrycka, Cécile Kashetu Kyenge, Marju Lauristin, Juan Fernando López Aguilar, Monica Macovei, Roberta Metsola, Péter Niedermüller, Soraya Post, Judith Sargentini, Birgit Sippel, Branislav Škripek, Sergei Stanishev, Helga Stevens, Traian Ungureanu, Bodil Valero, Marie-Christine Vergiat, Udo Voigt, Josef Weidenholzer, Kristina Winberg, Tomáš Zdechovský
Suplentes presentes no momento da votação final	Andrea Bocskor, Jeroen Lenaers, Nadine Morano, Morten Helveg Petersen, Emil Radev, Axel Voss
Suplentes (art. 200.º, n.º 2) presentes no momento da votação final	Josu Juaristi Abaunz, Georg Mayer

VOTAÇÃO NOMINAL FINAL NA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO

37	+
ALDE	Nathalie Griesbeck, Morten Helveg Petersen
ECR	Monica Macovei, Helga Stevens, Branislav Škripek
ENF	Georg Mayer
GUE/NGL	Josu Juaristi Abaunz, Marie-Christine Vergiat
PPE	Andrea Bocskor, Michał Boni, Agustín Díaz de Mera García Consuegra, Kinga Gál, Monika Hohlmeier, Barbara Kudrycka, Jeroen Lenaers, Roberta Metsola, Nadine Morano, Emil Radev, Traian Ungureanu, Axel Voss, Tomáš Zdechovský
S&D	Caterina Chinnici, Tanja Fajon, Ana Gomes, Sylvie Guillaume, Cécile Kashetu Kyenge, Dietmar Köster, Marju Lauristin, Juan Fernando López Aguilar, Péter Niedermüller, Soraya Post, Birgit Sippel, Sergei Stanishev, Josef Weidenholzer
Verts/ALE	Eva Joly, Judith Sargentini, Bodil Valero

1	-
NI	Udo Voigt

1	0
EFDD	Kristina Winberg

Legenda dos símbolos utilizados:
+ : a favor
- : contra
0 : abstenções