A vigilância por serviços de informações: salvaguardas dos direitos fundamentais e meios de defesa na União Europeia

Resumo

O artigo 7.º da Carta dos Direitos Fundamentais da União Europeia garante a todos os indivíduos na União Europeia (UE) o respeito pela vida privada e familiar, ao passo que o artigo 8.º garante o direito à proteção de dados pessoais. O artigo requer que tais dados sejam objeto de um tratamento leal para fins específicos e assegura o direito de acesso de cada pessoa aos seus dados pessoais, bem como o direito à retificação de tais dados. Também estipula que uma autoridade independente tem de regular a fiscalização do cumprimento deste direito. O artigo 47.º assegura o direito à ação, incluindo que a sua causa seja julgada de forma equitativa publicamente e num prazo razoável.

Quando a comunicação social do mundo inteiro começou a publicar os «documentos Snowden» em junho de 2013, foi tornada pública a existência de programas de vigilância global por parte de serviços de informações. As revelações Snowden não foram as primeiras suspeitas da existência de programas de vigilância de comunicações em larga escala criados no seguimento dos ataques de 11 de setembro de 2001. A vasta magnitude destas revelações, no entanto, permanece sem precedentes, potencialmente afetando a privacidade das pessoas pelo mundo. A vigilância deixou de visar meramente segredos empresariais ou de Estado, mas abrange a interceção das comunicações das pessoas em grande escala. Isso interfere quer com o respeito pela vida familiar e privada de indivíduos quer com o direito à privacidade e à proteção de dados — ambos salvaguardados ao nível da União Europeia pela Carta dos Direitos Fundamentais da União Europeia (a Carta). Enquanto tal, a UE e os seus Estados-Membros têm a obrigação de os proteger, incluindo no contexto da vigilância, e de fornecer às vítimas os meios de defesa para contestar a vigilância ilegal.

«Uma tal vigilância em larga escala e não dirigida é desproporcionada por natureza e constitui uma ingerência injustificada nos direitos garantidos pelos artigos 7.º e 8.º da Carta.»
(TJUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, conclusões do advogado-geral, 23 de setembro de 2015)

As revelações desencadearam uma diversidade de reações. Na comunidade das agências de informações, em particular no seio de organismos especializados responsáveis por fiscalizar serviços de informações, foram realizados investigações e relatórios específicos sobre as revelações Snowden que escrutinaram ainda mais as respetivas implicações. As instituições da UE reagiram vigorosamente. A Comissão Europeia, o Conselho da União Europeia e o Parlamento Europeu elaboraram relatórios sobre as revelações, expressaram preocupação acerca de programas de vigilância em larga escala, buscaram clarificações da parte das autoridades dos Estados Unidos, e trabalharam para «reconstruir a confiança» nas relações EUA-UE. Apesar de ainda ser cedo para aferir o pleno impacto das revelações Snowden, as investigações pós-Snowden em alguns Estados-Membros da UE concluíram que os respetivos quadros jurídicos nacionais atuais carecem de reformas. Tal foi igualmente sublinhado pela Resolução do Parlamento Europeu de março de 2014 sobre o programa de vigilância da Agência Nacional de Segurança dos Estados Unidos (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da União Europeia

e na cooperação transatlântica no domínio da justiça e dos assuntos internos [2013/2188(INI), P7_TA (2014)0230], que lança um *Habeas Corpus Digital Europeu*.

«As revelações Snowden dão-nos uma oportunidade para agir. Espero que transformemos aquelas reações em algo positivo e duradouro que se prolongue no próximo mandato deste Parlamento, nomeadamente numa carta de direitos de proteção de dados da qual todos nos possamos orgulhar.»
(Claude Moraes, deputado ao Parlamento Europeu, Relator na investigação NSA do PE, comunicado de imprensa, 12 de março de 2014)

Mapeamento dos quadros jurídicos dos Estados-Membros da União Europeia relativos à vigilância

Em abril de 2014, o Parlamento Europeu solicitou à Agência dos Direitos Fundamentais da União Europeia (FRA) que realizasse «uma investigação aprofundada sobre a proteção dos direitos fundamentais no contexto da vigilância». A FRA assim fez, mapeando os quadros jurídicos dos 28 Estados-Membros da União Europeia relativos à vigilância e fornecendo uma visão global dos padrões de direitos fundamentais existentes. Focou-se nos mecanismos de supervisão e nos meios de defesa ao dispor dos indivíduos que alegassem violações do seu direito à privacidade.

A pesquisa jurídica da FRA não examina as técnicas de vigilância enquanto tais. A pesquisa revê o modo como os atuais quadros jurídicos permitem o uso de tais técnicas, e explora o papel crucial que os organismos especializados desempenham na supervisão do trabalho dos serviços de informações.

Além disso, escrutina em que medida as salvaguardas relevantes protegem a privacidade e a proteção de dados em todos os 28 Estados-Membros da União Europeia.

Os «serviços de informações» têm um mandato externo e focam-se em ameaças externas, ao passo que os «serviços de segurança» têm um mandato interno e se focam em ameaças internas. O relatório da FRA refere-se a «serviços de informações» enquanto termo genérico para ambos.

Este resumo apresenta as principais conclusões da FRA, que são publicadas na íntegra no relatório intitulado *A vigilância por serviços de informações: salvaguardas de direitos fundamentais e meios de defesa na União Europeia — Mapeamento dos quadros jurídicos dos Estados-Membros* (ver Informações adicionais).

Recolha de dados e cobertura

Para esta pesquisa, a FRA examinou os quadros jurídicos relativos à vigilância nos 28 Estados-Membros da União Europeia, analisando as normas e os padrões de direitos fundamentais relevantes a fim de apresentar uma análise comparativa do contexto jurídico da vigilância em toda a União.

Com base em respostas fornecidas pela Franet, a rede de pesquisa multidisciplinar da agência, a FRA recolheu dados e informação através de pesquisa documental em todos os 28 Estados-Membros da União Europeia. Foram reunidas informações adicionais através de trocas com parceiros-chave, incluindo um conjunto de oficiais de ligação da FRA nos Estados-Membros, organismos especializados e peritos individuais. As conclusões também se baseiam em publicações e relatórios existentes que visam apoiar os legisladores nacionais a criar os quadros jurídicos para os serviços de informações e a sua supervisão democrática.

Um segundo relatório sociojurídico com as conclusões da FRA, baseado em pesquisa empírica, será publicado numa fase posterior, continuando a aprofundar os resultados ora apresentados.

As salvaguardas dos direitos fundamentais e o direito da União Europeia

«A dura verdade é que a utilização de tecnologia de vigilância em larga escala efetivamente suprime por completo o direito à privacidade das comunicações na Internet.»
[Organização das Nações Unidas, relator especial das Nações Unidas para a promoção e a defesa dos direitos do Homem e das liberdades fundamentais no âmbito da luta contra o terrorismo (2014), quarto relatório anual apresentado à Assembleia Geral, A/69/397, de 23 de setembro de 2014]

Os Estados-Membros da União Europeia encontram-se todos vinculados a padrões mínimos de direito internacional dos direitos humanos desenvolvidos pela Organização das Nações Unidas (ONU), que têm aplicabilidade universal, tais como a resolução do Conselho de Direitos Humanos sobre o direito à privacidade na era digital (Doc. A/HRC/28/L.27, de 24 de março de 2015). Diversos organismos especializados e decorrentes de tratado da ONU condenaram as práticas de vigilância em larga escala no seguimento das revelações Snowden. As normas do Conselho da Europa, incluindo a jurisprudência Tribunal Europeu dos Direitos do Homem (TEDH), também estabelecem padrões mínimos. Acresce que o direito da União Europeia, tal como interpretado pelo Tribunal de Justiça da União Europeia (TJUE), é relevante. Finalmente, numa área em que apenas é diretamente aplicável regulamentação internacional limitada — que não configura o atual direito internacional sobre direitos do Homem —, as medidas de autorregulamentação e o direito não vinculativo também são importantes.

O relatório foca-se nos direitos à privacidade e à proteção de dados, que estão estabelecidos nos artigos 7.º e 8.º da Carta. O direito à proteção de dados também está estabelecido no direito da União Europeia primário e secundário, assegurando que, no seu respetivo âmbito de aplicação, o processamento de dados pessoais é efetuado de modo legal e apenas na extensão necessária ao cumprimento do legítimo objetivo prosseguido. Estes direitos estendem-se a todas as pessoas, quer sejam cidadãos da UE, quer de países terceiros. Em conformidade com artigo 52.º, n.º 1, da Carta, qualquer limite a este direito tem de ser necessário e proporcional, tem de ir genuinamente ao encontro de objetivos de interesse geral reconhecidos pela União, tem de ser fornecido pelo direito e tem de respeitar a essência de tais direitos.

Apesar da existência de linhas diretrizes internacionais, não existe um entendimento uniforme de «segurança nacional» em toda a União Europeia. Nem a legislação da UE nem a jurisprudência do TJUE definem este conceito, apesar de o TJUE ter afirmado que as exceções aos direitos fundamentais têm de ser justificadas e interpretadas de modo limitado.

Esta delineação ambígua de «segurança nacional» tem repercussões para a aplicabilidade do direito da União Europeia. O artigo 4.º, n.º 2, do Tratado da União Europeia estabelece que «a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro». Tal não significa que a exceção da «segurança nacional» torna o direito da UE inaplicável. A interpretação da «segurança nacional» ao nível dos Estados-Membros e o modo como os programas de vigilância são implementados pode ser avaliado pelas instituições da União Europeia, sobretudo pelo TJUE.

Tipos de vigilância: dirigida e não-dirigida

A pesquisa da FRA examina como é que a vigilância, quer dirigida quer não-dirigida, é organizada nos termos dos quadros jurídicos dos Estados-Membros da União Europeia.

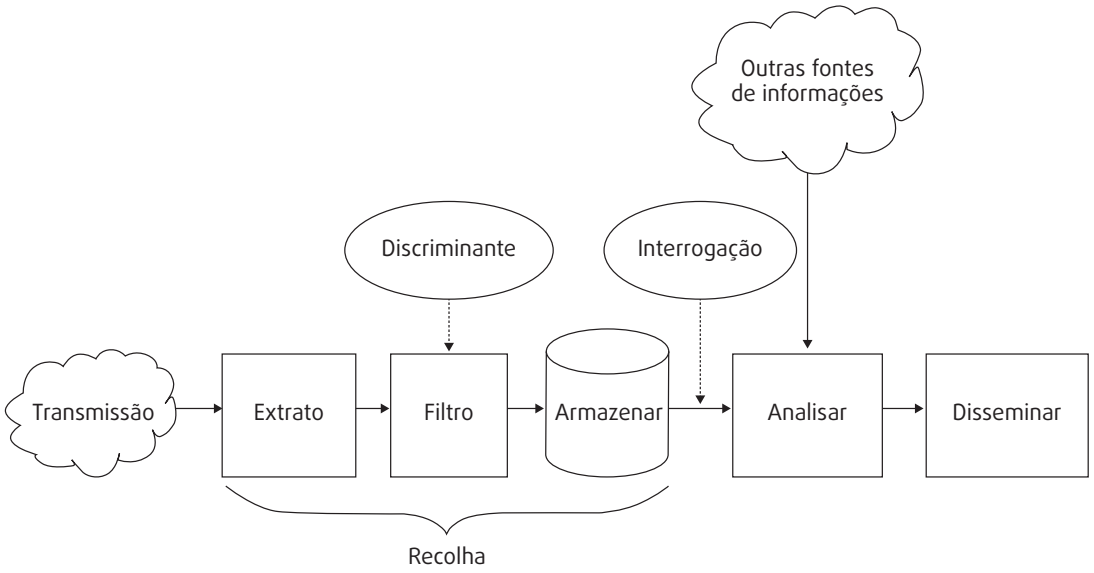
O Comité de Revisão neerlandês para os Serviços de Segurança e de Informação (CTIVD) define a vigilância dirigida e não-dirigida nos seguintes termos:

- a interceção direcionada refere-se à «[i]nterceção em que a pessoa, organização ou característica técnica face à qual a recolha de dados seja dirigida possa ser especificada previamente»;
- a interceção não direcionada refere-se à «[i]nterceção em que a pessoa, organização ou característica técnica face à qual a recolha de dados seja dirigida não possa ser especificada previamente».

CTIVD, *Relatório Anual 2013–2014*, Haia, 31 de março de 2014, p. 45–46.

A vasta escala dos dados recolhidos através dos programas de vigilância revelados — tais como PRISM, Xkeyscore e Upstream — desencadearam vastas reações. A «vigilância em larga escala» (frequentemente entendida como não-dirigida) implica a recolha de volumes de dados amplamente diferentes

Figura — Modelo conceptual de informações sobre transmissões



Fonte: Estados Unidos, Conselho Nacional de Pesquisa (2015), p. 28.

dos recolhidos através de métodos de vigilância tradicionais, secretos (dirigidos), tais como escutas telefónicas. Este último é baseado em prévia suspeita face a um indivíduo ou uma organização em específico. Este tipo de vigilância tem prevalência e é reconhecido pela legislação dos Estados-Membros da União Europeia. A esmagadora maioria dos quadros jurídicos dos Estados-Membros da União Europeia não regula nem sequer refere a «vigilância em larga escala» enquanto tal. Apenas alguns Estados-Membros da União Europeia possuem legislação detalhada acerca de «informações sobre transmissões» (SIGINT), que é o termo genérico utilizado para descrever a interceção pelos serviços de informações de sinais provenientes de várias fontes. A pesquisa da FRA utiliza o termo «informações sobre transmissões» ao longo da sua análise.

A SIGINT deriva das informações militares. Refere-se à coleção automatizada de informação através da interceção e recolha de dados digitais relativos à atividade de informações. A figura sublinha que os sinais recolhidos são filtrados utilizando discriminantes ou seletores — um conjunto de parâmetros colocados no processo de filtragem, ou *a priori* ou de modo dinâmico, para definir os critérios que determinarão quais os dados a armazenar de forma a obter a informação relevante (por exemplo, «todos os endereços de correio eletrónico utilizados em comunicações com o Iémen»).

O Conselho Nacional de Pesquisa das Academias Nacionais dos Estados Unidos referiu-se às informações sobre transmissões como um termo englobante de quaisquer dados armazenados num dispositivo eletrónico. A Comissão de Veneza utiliza SIGINT enquanto termo coletivo para meios e métodos de interceção e análise de comunicações rádio (incluindo telefonia celular e via satélite) e por cabo.

A análise da FRA dos quadros jurídicos que regulam os métodos de vigilância dos serviços de informações demonstra que a legislação de cinco Estados-Membros da União Europeia (França, Alemanha, Países Baixos, Suécia e Reino Unido) detalham as condições que permitem a utilização de vigilância quer dirigida, quer não dirigida, tal como informações sobre transmissões. Outra legislação de Estados-Membros especifica de modo insuficiente estas condições, obstando a uma análise jurídica dos exatos procedimentos em vigor sobre a recolha de informações sobre transmissões. Ainda que a legislação nestes países não se refira especificamente a SIGINT, a mesma pode todavia ser implementada. No entanto, dado que a prática é apenas prescrita em medidas regulamentares não publicadas nestes países, uma análise dos quadros jurídicos aplicáveis não elucidará sobre a questão.

Principais resultados

Os serviços de informações e a legislação sobre vigilância

Objetivo e estrutura dos serviços de informações

O principal objetivo dos serviços de informações em sociedades democráticas é proteger a segurança nacional e os valores fundamentais de uma sociedade aberta mediante a utilização de ferramentas de informações secretas. A organização da comunidade das agências de informações em cada Estado-Membro da União Europeia está estreitamente ligada a desenvolvimentos históricos específicos do país, e não se rege necessariamente por padrões de direitos fundamentais. Consequentemente, os serviços de informações são criados de modos extremamente diversos em toda a UE. Em alguns Estados-Membros, dois serviços de informações realizam o trabalho, enquanto noutros há cinco ou seis organismos responsáveis.

- Quase todos os Estados-Membros da União Europeia estabeleceram pelo menos duas entidades de serviços de informações diferentes, uma para assuntos civis e outra para assuntos militares; a última não é abrangida pelo presente relatório. Os serviços de informações civis são geralmente subordinados dos ministérios dos assuntos internos, e por vezes também do primeiro-ministro ou do presidente.

- Em alguns Estados-Membros, os serviços civis estão ainda subdivididos num serviço com um mandato interno e noutro com um mandato externo. Aliás, alguns Estados-Membros confiaram medidas de informações a unidades especializadas numa ameaça em particular, tal como o crime organizado, corrupção ou luta contra o terrorismo.

Proteger a segurança nacional

A pesquisa da FRA examina a noção de «segurança nacional» à luz do mandato dos serviços de informações e das medidas de vigilância que estes possam implementar. Mais uma vez as conclusões revelam grande diversidade entre os Estados-Membros da União Europeia.

- O principal objetivo dos serviços de informações é proteger a segurança nacional, mas o conceito não está harmonizado em todos os Estados-Membros da União Europeia. O âmbito da segurança nacional raramente é definido, e por vezes são utilizados termos similares. Outros Estados-Membros não utilizam de todo o termo «segurança nacional», referindo, por outro lado, termos como «segurança interna» e/ou «segurança externa», ou «segurança do Estado».

- O âmbito das várias tarefas dos serviços de informações (isto é, o seu mandato) não é idêntico em todos os Estados-Membros da União Europeia. Além das áreas mais tradicionais, os mandatos de alguns serviços de informações incluem o crime organizado e o cibercrime. Estes termos não se encontram definidos de modo harmonioso.

Regulamentação legal da vigilância

A distinção entre as tarefas de manutenção da ordem pública e as dos serviços de informações nem sempre é clara. Qualquer expansão de tarefas tem de ser apropriadamente justificada como necessária para salvaguardar o Estado, que é a razão subjacente ao estabelecimento de serviços de informações.

- A maioria dos quadros jurídicos dos Estados-Membros apenas regula a vigilância dirigida, quer de indivíduos quer de grupos/organizações definidos/as. Além de lidarem com a vigilância dirigida, cinco Estados-Membros aprovaram legislação detalhada sobre as condições para utilizar informações sobre transmissões.

- Olhando para os padrões de direitos humanos aplicáveis, os quadros jurídicos nacionais são omissos quanto a definições claras que indiquem as categorias de pessoas e o âmbito das atividades que podem ser objeto de recolha de informações.

- Os serviços de informações são regulados por lei na vasta maioria dos Estados-Membros (26 em 28). As disposições legais regulam a organização e o funcionamento dos serviços de informações dos países. A Constituição de um Estado-Membro proíbe o respetivo serviço de informações de realizar vigilância. Outro Estado-Membro está em vias de aprovar legislação que irá regulamentar as práticas dos seus serviços de informações.

- A análise da FRA mostra que a base jurídica em que assentam os mandatos e os poderes dos serviços de informações nacionais nos Estados-Membros da União Europeia vão desde uma legislação única que rege a organização e os meios dos serviços nacionais até quadros complexos consistindo em diversa legislação e portarias que regulamentam aspetos específicos do seu mandato, da sua organização, das suas competências ou dos seus meios.

- A maioria dos Estados-Membros organiza o trabalho dos serviços de informações em duas legislações: uma sobre o mandato e organização do serviço, e outra sobre os meios de ação e as condições para os utilizar.

- A maioria dos Estados-Membros da União Europeia (23 em 28) possuem serviços de informações separados das autoridades de manutenção da ordem pública. Dois Estados-Membros afastaram-se recentemente de sistemas em que os serviços de informações pertenciam à polícia ou a autoridades de manutenção da ordem pública semelhantes.

Supervisão dos serviços de informações

A análise da FRA debruça-se sobre os mecanismos de responsabilidade relacionados com a vigilância realizada por serviços de informações. Em particular, a mesma descreve o modo como os Estados-Membros da União Europeia estabeleceram mecanismos de supervisão. A supervisão é um meio de assegurar a responsabilidade pública pelas decisões e ações dos serviços de informações. De acordo com os peritos, a supervisão visa evitar o abuso de poder, legitimar o exercício de poderes intrusivos e lograr um resultado melhor após uma avaliação de ações específicas. O consenso geral, retirado de um relatório da Comissão de Veneza e outros estudos académicos, é que a supervisão deve ser uma conjugação de:

- controlo executivo;
- supervisão preliminar;
- organismos compostos por peritos;
- controlo jurisdicional.

Controlo executivo e coordenação entre organismos de supervisão

O poder executivo pode controlar os serviços de informações de várias formas: especificando as suas prioridades e políticas estratégicas, ou estabelecendo linhas diretrizes; nomeando e /ou designando a direção superior do serviço; formulando o orçamento que o parlamento votará em última instância; ou aprovando a cooperação com outros serviços. O executivo também desempenha um papel crucial na autorização de medidas de vigilância em alguns Estados-Membros.

A supervisão efetiva requer uma coordenação apropriada entre os diversos organismos de supervisão a fim de assegurar que todos os aspetos do trabalho dos serviços de informações são abrangidos. Se os organismos de supervisão não dispuserem de um entendimento claro e abrangente do trabalho da comunidade das agências de informações por inteiro, surgirão lacunas na supervisão, e a efetividade do sistema de supervisão como um todo será dificultada.

- A diversidade entre os Estados-Membros da União Europeia em termos de sistemas políticos e jurídicos traduziu-se numa grande variedade de organismos que supervisionam os serviços de informações. Os Estados-Membros da União Europeia possuem sistemas de supervisão amplamente diferentes. Se bem que há boas práticas a retirar dos sistemas em vigor, algumas áreas individuais beneficiariam de reformas legais que reforçaram o poder dos organismos de supervisão.

- É concedida uma grande variedade de poderes aos vários organismos de supervisão, variando também a medida em que os mesmos podem exercer estes poderes.

- Sete Estados-Membros possuem sistemas de supervisão que conjugam o executivo, o parlamento, o poder judicial (por via de aprovação *ex ante*) e organismos compostos por peritos. No entanto, estes não incluem nenhum dos países que possuem quadros jurídicos que permitem a recolha de informações sobre transmissões.

- A supervisão efetiva não requer necessariamente todos os quatro tipos de mecanismos de supervisão. Uma tal supervisão pode ser conseguida se os organismos existentes se complementarem mutuamente e, no seu todo, formarem um sistema forte capaz de avaliar se o mandato dos serviços de informações é implementado devidamente. Tal ocorrerá se os poderes de supervisão cobrirem todas as áreas de atividade de um serviço de informações. No

entanto, sempre que o próprio mandato seja dúbio ou insuficientemente desenvolvido, os organismos de supervisão não serão capazes de exercer qualquer influência.

- O acesso à informação e a documentos por parte dos organismos de supervisão é essencial. Se bem que a informação reunida por serviços de informações é sensível, e as salvaguardas têm de garantir que a mesma será tratada em conformidade, os organismos de supervisão não podem desempenhar as suas tarefas sem primeiro ter acesso a toda a informação relevante. O contrário, no entanto, parece ser a norma.

Supervisão parlamentar

A supervisão parlamentar é importante dada a responsabilidade do parlamento no que respeita à responsabilização do governo. O parlamento, enquanto legislador, é responsável por aprovar legislação clara e acessível, que estabeleça os serviços de informações e especifique a sua organização, poderes especiais e limitações. Também é responsável pela aprovação do orçamento dos serviços de informações, e nalguns Estados-Membros escrutina se as suas operações estão em linha com o quadro jurídico.

- As conclusões da FRA mostram que 24 Estados-Membros da União Europeia incluem supervisão parlamentar; em 21 de entre estes há comissões parlamentares especiais que supervisionam os serviços de informações. Alguns Estados-Membros criaram uma comissão parlamentar para lidar com os diversos serviços de informações e de segurança, ao passo que outros criaram diversas comissões para lidar com os serviços de modo individual.

- Nenhuma comissão parlamentar de um Estado-Membro possui acesso sem restrições à informação de serviços de informações.

- As diferentes comissões parlamentares nos Estados-Membros têm mandatos variáveis: a maioria tem poderes de supervisão tradicionais relacionados com a legislação, o orçamento e a receção de informação sobre a função dos serviços, ao passo que um número muito reduzido pode receber queixas, adotar decisões vinculativas para os serviços de informações ou auxiliar na aprovação de medidas de vigilância.

- No que respeita ao poder das comissões parlamentares para iniciar investigações, a legislação da maioria dos países autoriza estas comissões a requerer informação aos serviços de informações ou ao executivo, mas não a exigi-la.

Supervisão por peritos

A supervisão por peritos é excecionalmente valiosa porque permite a indivíduos familiarizados com o tema, que têm tempo para dedicar à matéria e que são independentes de obediências políticas, escrutinar as ações dos serviços de informações. De acordo com o Comissário para os Direitos Humanos do Conselho da Europa, aqueles indivíduos estão frequentemente melhor posicionados para levar a cabo a supervisão do dia-a-dia da atividade dos serviços de informações e de segurança.

- Muito embora a supervisão parlamentar seja crucial, a mesma carece de ser complementada por outros organismos de supervisão, em particular por organismos compostos por peritos fortes que possam supervisionar atividades operacionais, incluindo a recolha, troca e utilização de dados pessoais, bem como a proteção do direito à vida privada.

- Em toda a União Europeia, 15 Estados-Membros criaram um ou mais organismos compostos por peritos exclusivamente dedicados à supervisão de serviços de informações. As suas competências incluem autorizar medidas de vigilância, investigar queixas, solicitar documentos e informações aos serviços de informações, e fornecer aconselhamento ao executivo e/ou parlamento. A fim de maximizar o seu potencial, deve ser-lhes concedida independência, recursos e poderes adequados.

- Em alguns Estados-Membros, a autorização de medidas de vigilância não inclui nenhumas instituições que são independentes dos serviços de informações e do executivo.

- Nos Estados-Membros que têm um organismo independente para autorizar medidas de vigilância, a vigilância dirigida tende a carecer de autorização judicial, ao passo que a aprovação por via de organismos compostos por peritos é a outra solução preferida. Não existe uma abordagem comum à supervisão da recolha de informações sobre transmissões.

- Apesar de a compreensão dos aspetos jurídicos da vigilância ser indispensável, os organismos compostos por peritos também têm de ser tecnicamente competentes. Alguns Estados-Membros asseguram-se disto mesmo através da inclusão de peritos de vários domínios, incluindo as tecnologias da informação e comunicação (ICT). Outros apoiam-se fortemente numa conjugação de atuais e antigos juízes e deputados.

Nos Estados-Membros da União Europeia, as autoridades competentes em matéria de proteção de dados (DPA) — organismos especializados chamados a salvaguardar a privacidade e a proteção de dados — tem um papel fundamental na salvaguarda de dados pessoais. Este papel está consagrado no direito da União Europeia primário e secundário. Mas os organismos compostos por peritos especializados na supervisão de serviços de informações possuem sem dúvida conhecimento especializado reconhecido em matéria de privacidade e proteção de dados na área das informações.

- As conclusões da FRA mostram que, em comparação com outras atividades de processamento de dados e com os responsáveis pelo tratamento de dados do setor privado e público, em sete Estados-Membros as DPA têm os mesmos poderes sobre os serviços de informações que todos os outros responsáveis pelo tratamento de dados. Em 12 Estados-Membros, as DPA não têm competência sobre os serviços de informações, e em nove os seus poderes são limitados.

- Nos Estados-Membros em que as DPA e os outros organismos de supervisão compostos por peritos partilham competências, uma falta de cooperação entre estes poderá deixar lacunas resultantes de responsabilidades fragmentadas. Nos Estados-Membros em que as DPA não têm competência sobre os serviços de informações, o organismo de supervisão é responsável por se assegurar que as salvaguardas de privacidade e de proteção de dados são devidamente aplicadas.

- Pesquisa anterior da FRA na área do acesso a meios de defesa de proteção de dados identifica a necessidade de melhorar a capacidade das DPA; é importante tendo em vista o papel que as DPA podem desempenhar na supervisão de serviços de informações.

Meios de defesa

Em conformidade com os padrões internacionais aplicáveis, quem suspeitar que é vítima de uma violação de proteção de dados ou de privacidade tem de ter uma oportunidade de procurar solucionar a situação. O direito à ação — que permite aos indivíduos obterem reparação legal devido a uma violação dos seus direitos — é uma componente essencial do acesso à justiça. Um meio de defesa tem de ser «efetivo» na prática e na legislação.

Tal como mostram relatórios anteriores da FRA sobre o acesso a meios de defesa de proteção de dados e sobre o acesso à justiça, estão ao dispor das vítimas de violações de proteção de dados e de privacidade diversas formas de tutela. Os organismos não judiciais desempenham um papel de tutela importante na área da vigilância, dadas as dificuldades práticas no acesso aos tribunais comuns. Os organismos não judiciais em todos os 28 Estados--Membros da União Europeia incluem organismos parlamentares, executivos e compostos por peritos (incluindo DPA), bem como provedorias. Em alguns Estados-Membros, o número de organismos não judiciais com papéis de tutela na área da vigilância é relativamente encorajador, mas deve ser visto à luz das seguintes conclusões.

Nem a complexidade do panorama da tutela, nem o volume de informação recolhido pelos serviços de informações que realizam SIGINT facilitam a implementação de meios de defesa efetivos. A fragmentação e a compartimentação das diferentes formas de tutela tornaram difícil a procura de meios de defesa. Na verdade, os dados recolhidos mostram que apenas um número limitado de casos em que se contestam práticas de vigilância foram julgados ao nível nacional desde as revelações Snowden.

Obrigação de informar e o direito de acesso

O direito a ser notificado e de acesso à informação é crucial para alertar os indivíduos para as medidas de vigilância e para iniciar uma ação de tutela. No entanto, o Tribunal Europeu dos Direitos do Homem (TEDH) aceitou que estes direitos podem ser limitados mediante justificação (ver TEDH, *Klass e Outros c. Alemanha*, N.º 5029/71, 6 de setembro de 1978). As conclusões da FRA mostram que o secretismo em torno do trabalho dos serviços de informações limita efetivamente estes direitos. Outro fator é o vasto volume de dados recolhido por meio de SIGINT comparado com formas mais tradicionais de vigilância.

- Em oito Estados-Membros, a obrigação de informar e o direito de acesso não estão de modo algum estabelecidos por lei; são aplicáveis as regras sobre documentos classificados ou sobre segredos de Estado. Nos outros 20 Estados-Membros, a legislação estabelece a obrigação de informar e o direito de acesso, em alguns casos dentro de prazos específicos, apesar de sujeito a restrições. Estas restrições incluem diversas fundamentações, tais como a segurança nacional, interesses nacionais ou a finalidade da própria medida de vigilância.

- Apenas dois Estados-Membros têm disposições específicas sobre a obrigação de informar no contexto de informações sobre transmissões: num, os indivíduos não são informados se os seletores utilizados não forem diretamente atribuíveis ao indivíduo; noutro, o indivíduo não é informado se os dados pessoais obtidos forem

imediatamente eliminados após a recolha e não forem objeto de processamento adicional.

- Os organismos de supervisão de 10 Estados-Membros da União Europeia, incluindo seis DPA nacionais, revêm as restrições ao direito a ser informado e ao direito de acesso à informação através da verificação da razoabilidade da ameaça à segurança nacional invocada, e/ou através do exercício indireto do direito de acesso do indivíduo. No último caso, os organismos equacionam se o acesso aos dados pode ser concedido ou se a recusa em concedê-lo é legítima, e também escrutinam a legalidade do processamento dos dados. Num Estado-Membro, é necessário um mandado judicial — certificando que a notificação colocaria em perigo a investigação, ou a existência de outros argumentos contra a mesma.

- Dois outros Estados-Membros não concedem um direito de acesso à informação enquanto tal. No entanto, a legislação estabelece um direito que produz o mesmo resultado: um indivíduo pode solicitar que o organismo de supervisão verifique se os seus dados são objeto de vigilância ilegal.

- Em alguns Estados-Membros, o organismo de supervisão envolvido no exercício indireto do direito de solicitar o acesso à informação, nem confirma, nem nega o processamento de dados. As respostas são normalmente limitadas a declarar que a queixa foi recebida e/ou verificada.

Meios de defesa judiciais

Todos os Estados-Membros concedem aos indivíduos a oportunidade de apresentar queixa por violações de privacidade por via dos tribunais, independentemente das mesmas terem ocorrido ou não por força de vigilância dirigida ou por força de informações sobre transmissões. Os tribunais constituem uma via para os indivíduos se queixarem acerca de interferências na sua privacidade, inclusive contestando decisões de organismos de supervisão sobre as suas alegações quanto a violações de privacidade. Também concedem aos indivíduos uma oportunidade de obterem tutela — inclusivamente na área da vigilância.

- No entanto, a pesquisa anterior da FRA identificou a falta de especialização dos juízes em matéria de proteção de dados como um obstáculo sério a tutelar efetivamente as situações de violação de proteção de dados. Esta conclusão é relevante para a vigilância, onde, para além do secretismo necessário ligado às informações, é essencial, por exemplo, um conhecimento especializado relevante em ICT ou em informações.

- Apenas dois Estados-Membros mitigaram a falta de especialização com respeito a meios de defesa por meio do envolvimento dos juízes/tribunais que quer tenham os conhecimentos necessários à sua disposição para decidir (frequentemente) sobre matérias técnicas, quer tenham autorização para aceder a material secreto.

Meios de defesa não judiciais

As opções não judiciais são habitualmente mais acessíveis aos indivíduos do que os mecanismos judiciais porque as normas processuais são menos rígidas, a apresentação de queixa é menos onerosa e os trâmites são mais rápidos. Indícios anteriores da FRA confirmam-no, em particular no contexto da proteção de dados, já que um maior número de queixas tende a ser apresentada junto de DPA nacionais e apenas algumas queixas seguem trâmites judiciais. No entanto, o número de organismos não judiciais — distintos das DPA — que, de acordo com os dados, atuam na área da proteção de dados é reduzido, e muitos organismos não judiciais apenas têm poder limitado para disponibilizar meios de defesa.

- Os organismos de supervisão (incluindo DPA) responsáveis por lidar com queixas são instituições independentes na grande maioria dos Estados-Membros.

- Nos casos em que um organismo de supervisão executivo tem poderes de tutela, a questão da independência coloca-se quando também tem poder para decidir em matéria de vigilância. Os organismos de supervisão parlamentares e os compostos por peritos tem mais estruturas administrativas autónomas — mas a autonomia não garante um meio de defesa efetivo a menos que também seja apoiada por conhecimentos suficientes. O modo como os membros dos organismos de supervisão são nomeados e a sua posição na hierarquia administrativa também são aspetos importantes a considerar ao equacionar a independência de um organismo.

- Treze DPA em Estados-Membros da União Europeia têm o poder de examinar queixas individuais e emitir decisões vinculativas. Mas em três destas, o poder para aceder a ficheiros e instalações é limitado. Em cinco Estados-Membros, aplicam-se requisitos adicionais — requerer a presença do dirigente ou de um membro da DPA durante inspeções em instalações de serviço de informações.

- Cinco dos sete Estados-Membros que confiam aos seus organismos de supervisão compostos por peritos (que não sejam DPA) poderes de tutela específicos, fazem-no por meio de uma autorização a que estes organismos emitam decisões vinculativas. Em dois Estados-Membros da União Europeia, um organismo de supervisão executivo tem poderes de tutela. As comissões parlamentares em quatro Estados-Membros têm competência em matéria de queixas individuais, mas apenas uma pode resolvê-las por meio de decisões vinculativas.

- As provedorias, que existem em todos os 28 Estados-Membros da União Europeia, maioritariamente lidam com falhas administrativas ao invés de lidar com a legitimidade concreta da vigilância. Apenas um Estado-Membro estabelece poderes de tutela para a provedoria por via da relevante legislação em matéria de informações. Acresce que os poderes das provedorias podem ser bastante limitados, e os trâmites tipicamente terminam com recomendações não vinculativas que visam corrigir a situação e orientar ações futuras, ao invés de terminarem com uma decisão vinculativa, com força executiva. Tal atinge obviamente a efetividade dos meios de defesa que são capazes de fornecer.

- Outros elementos que podem facilitar o acesso do individuo aos meios de defesa incluem regras mais flexíveis sobre o ônus da prova e ações coletivas, bem como proteção efetiva para denunciantes. A Assembleia Parlamentar do Conselho da Europa considera a denúncia de irregularidades como a ferramenta mais eficaz para fazer cumprir os limites colocados à vigilância.

Conclusões

Ao lidar com uma área de competência restrita da União Europeia, o relatório sublinha a diversidade entre Estados-Membros no que respeita ao modo como os serviços de informações estão organizados e desempenham as suas tarefas essenciais.

As medidas de vigilância interferem em grande medida nos direitos dos indivíduos. Dada a sua natureza secreta, os indivíduos estão obrigados a valer-se de um grau de confiança nas autoridades públicas, que por sua vez estão obrigados a salvaguardar os direitos fundamentais dos indivíduos. Atingir o nível de confiança que uma sociedade deve ter perante os respetivos serviços de informações requer responsabilização. Legislação clara e acessível, mecanismos de supervisão fortes, mecanismos de controlo apropriados e meios de defesa efetivos são apenas alguns dos elementos essenciais para atingir este tipo de responsabilização, o que indubitavelmente permanece difícil devido ao secretismo em que operam os serviços de informações. Apresentar e manter legislação clara e acessível e mecanismos de supervisão fortes ao nível dos Estados-Membros constitui apenas o primeiro passo na direção de um sistema transparente e consentâneo com os direitos fundamentais — as dificuldades neste sentido sugerem a permanência de obstáculos.

As reações às revelações Snowden realçaram a necessidade de adaptar e fortalecer os quadros jurídicos relevantes na União Europeia e em todos os seus Estados-Membros. A pesquisa da FRA demonstra que um número de reformas jurídicas foram já implementadas. Avaliações periódicas do funcionamento e da legitimidade dos quadros que regem a atividade de serviços de informações tem de se tornar parte integrante dos sistemas de supervisão. Como aprofundar a reforma dos quadros jurídicos que lidam com a falta de supervisão adequada é também uma questão-chave. Acresce que as reformas nos Estados-Membros da União Europeia têm de ter em consideração os recentes desenvolvimentos tecnológicos para assegurar que os mecanismos de supervisão são dotados dos instrumentos e dos conhecimentos especializados necessários. Conseguir tudo isto é sem dúvida desafiante, mas é vital para realizar a difícil tarefa de proteger a segurança ao passo que se salvaguardam os direitos fundamentais.

Proteger o público das ameaças à segurança e salvaguardar os direitos fundamentais implica um equilíbrio delicado. Atentados brutais e inovações tecnológicas que tornam possível a monitorização em larga escala de dados comunicações complicaram ainda mais a questão, desencadeando preocupações acerca da violação dos direitos à privacidade e à proteção de dados em nome da proteção da segurança nacional. As revelações Snowden, que descobriram esforços globais de vigilância indiscriminada e extensa, tornam claro que são necessárias salvaguardas reforçadas destes direitos.

Este relatório, redigido em resposta ao apelo do Parlamento Europeu para pesquisa pormenorizada sobre proteção de direitos fundamentais no contexto da vigilância, faz um mapeamento e analisa os quadros jurídicos sobre vigilância em vigor nos Estados-Membros da União Europeia. Centrado na chamada «vigilância em larga escala», apresenta também pormenorizadamente os mecanismos de supervisão introduzidos em toda a União Europeia, enuncia o trabalho de entidades encarregues da supervisão dos esforços de vigilância e apresenta os meios de defesa ao dispor de indivíduos que procurem contestar tal atividade de informações. Ao demonstrar as considerações complexas em causa, o presente relatório sublinha o quão difícil pode ser lidar com o que muitas vezes é visto como sendo prioridades concorrentes e contribui para o debate em curso acerca de saber como melhor as reconciliar.

Informações adicionais:

Para aceder ao relatório completo da FRA *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* (A vigilância por serviços de informações: salvaguardas dos direitos fundamentais e meios de defesa na União Europeia — Mapeamento dos quadros jurídicos dos Estados-Membros), consulte http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

Consultar também outras publicações da FRA nesta matéria:

- FRA-Conselho da Europa (2014), *Manual da Legislação Europeia sobre Proteção de Dados*, Luxemburgo, Serviço das Publicações, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (disponível em línguas da UE)
- FRA (2014), *Access to data protection remedies in EU Member States* (Acesso a vias de recurso em matéria de proteção de dados nos Estados-Membros da União Europeia), Luxemburgo, Serviço das Publicações, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states e a síntese http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary (disponível em línguas da União Europeia)

Uma visão global das atividades da FRA em matéria de proteção de dados está disponível em: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Serviço das Publicações

FRA — AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA

Schwarzenbergplatz 11 – 1040 Viena – Áustria
Tel. +43 158030-0 – Fax: +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Print: ISBN 978-92-9491-028-8, doi:10.2811/76794
PDF: ISBN 978-92-9491-030-1, doi:10.2811/63847

TK-04-15-738-PT-C (print); TK-04-15-738-PT-N (PDF)