Conselho da
União Europeia

Bruxelas, 31 de maio de 2024
(OR. en)

10477/24

LIMITE

COSI 102
ENFOPOL 268
IXIM 145
CATS 48
COPEN 289
CYBER 177

NOTA

de:	Presidência
para:	Comité de Representantes Permanentes/Conselho
Assunto:	Acesso aos dados para uma aplicação eficaz da lei: apresentação das recomendações do Grupo de Alto Nível – *Troca de pontos de vista*

1. Segurança interna na era digital

A transformação digital das nossas sociedades tem enorme potencial em termos de contributo para uma vida melhor, mais próspera e mais segura. Maximizar os benefícios da era digital para os cidadãos significa também minimizar as oportunidades que esta cria para a criminalidade grave e organizada, e para o terrorismo.

Na Europa, esta transformação digital deu origem a uma nova dimensão do espaço de liberdade, segurança e justiça sem fronteiras internas; um novo contexto em que a União Europeia promove e protege os valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos humanos. Garantir o direito dos europeus à segurança e à proteção exige um reforço da segurança interna europeia, nomeadamente através do desenvolvimento e da utilização de novas tecnologias seguras e centradas no ser humano, e da aplicação do princípio da segurança desde a conceção. A disponibilidade das provas eletrónicas e o acesso às mesmas é crucial para a prevenção, deteção, investigação e repressão da criminalidade grave e organizada exigem.

Atualmente, qualquer investigação e ação penal bem sucedida em casos de criminalidade grave ou organizada depende de provas eletrónicas. Paradoxalmente, embora a transformação digital tenha levado à criação, transmissão e armazenamento de um volume de dados cada vez maior, a disponibilidade de provas eletrónicas e o acesso às mesmas para fins de aplicação da lei e de justiça penal tornaram-se o principal desafio no que toca à proteção dos cidadãos da União contra a ameaça do terrorismo e da criminalidade grave e organizada.

Embora este desafio não seja novo, tem vindo a adquirir maior importância dia após dia. A aplicação da lei está literalmente «a ficar às escuras». Já em junho de 2017, o Conselho Europeu apelou a que se desse «*resposta aos desafios colocados por sistemas que permitem aos terroristas comunicar por meios a que as autoridades competentes não podem ter acesso, incluindo a criptografia de ponta a ponta, salvaguardando porém os benefícios que estes sistemas proporcionam em matéria de proteção da privacidade, dos dados e das comunicações*» e considerou que «*o acesso efetivo a meios de prova eletrónicos é essencial na luta contra a criminalidade grave e o terrorismo, e que a disponibilização dos dados deverá ser assegurada, desde que sujeita a garantias adequadas*»[1]. No seu acórdão de 30 de abril de 2024, o Tribunal de Justiça sublinhou, relativamente ao acesso a endereços IP no contexto de infrações penais cometidas em linha, que «*não permitir esse acesso comportaria [...] um risco real de impunidade sistémica* ... [de] *tipos de infrações penais cometidas em linha ou cuja prática ou preparação é facilitada pelas características próprias da Internet*»[2].

[1] Conclusões do Conselho Europeu de 22 e 23 de junho de 2017, ponto 2.
[2] Processo C-470/21, *La Quadrature du Net*, ponto 119.

2. Grupo de Alto Nível sobre o Acesso aos Dados para uma Aplicação Eficaz da Lei

A fim de identificar a via a seguir, a Presidência sueca, em cooperação com as Presidências espanhola e belga, lançou, em junho de 2023, o Grupo de Alto Nível (GAN) sobre o acesso aos dados para uma aplicação eficaz da lei, criado mediante decisão da Comissão de 6 de junho de 2023, composto por representantes dos Estados-Membros, da Comissão, dos órgãos e organismos competentes da UE e do Coordenador da UE da Luta Antiterrorista. Ao analisarem os desafios que os profissionais responsáveis pela aplicação da lei na União enfrentam no seu trabalho quotidiano, os peritos identificaram um conjunto de recomendações, incluídas no anexo da presente nota, destinadas a fazer face aos desafios atuais e previstos no contexto da evolução tecnológica, o que permite adotar uma abordagem abrangente da UE para assegurar a eficácia das investigações e ações penais enquanto elemento essencial do Estado de direito. As recomendações não são vinculativas, mas podem contribuir de forma significativa para fundamentar as escolhas políticas a nível nacional e da UE nos próximos anos.

As recomendações do GAN foram debatidas pelo Comité de Coordenação no domínio da Cooperação Policial e Judiciária em Matéria Penal (CATS), em 23 de maio de 2024, e pelo Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna (COSI), em 29 de maio de 2024, aquando da preparação da troca de pontos de vista no Conselho. Ambos os comités manifestaram o seu apoio ao procedimento do GAN e congratularam-se com o trabalho realizado pelos peritos.

O COSI identificou como possíveis principais questões prioritárias para a próxima legislatura:

1. O estabelecimento de regras para um acesso efetivo aos dados para fins de aplicação da lei que abranjam todos os prestadores de serviços de comunicações eletrónicas,

2. Um quadro legislativo harmonizado em matéria de conservação de dados para efeitos de aplicação da lei a nível da União, e

3. Soluções jurídicas e tecnicamente sólidas para aceder a dados cifrados em condições específicas, em casos individuais, sem um enfraquecimento geral da cifragem.

Poderia já fazer-se um levantamento da legislação e da jurisprudência em vigor. O COSI sugeriu que se iniciassem sem demora atividades nos domínios do reforço de capacidades, da normalização e da cooperação com a indústria, tirando o melhor partido das estruturas existentes e reforçando-as, incluindo o Polo da UE de Inovação para a Segurança Interna e as agências da UE. O COSI defendeu que, com base nas prioridades a definir pelo Conselho, deverá ser elaborado um roteiro que inclua um calendário claro e abranja aspetos financeiros. As delegações salientaram igualmente a necessidade de garantir a coordenação das atividades.

3. Perguntas dirigidas aos ministros

A Presidência convida os ministros a responderem às seguintes perguntas:

1. Quais são as três questões a que deverá ser dada prioridade durante a próxima legislatura?

2. Como poderão o Conselho e as suas estruturas apoiar a rápida execução das prioridades políticas da forma mais eficaz?

4. Sugestão de via a seguir

Convida-se o Conselho a tomar nota das recomendações do GAN sobre o acesso aos dados para uma aplicação eficaz da lei e a solicitar às próximas Presidências e à Comissão que levem por diante estes importantes trabalhos, com caráter prioritário.

ANEXO

Recomendações
do Grupo de Peritos de Alto Nível
sobre o Acesso aos Dados para uma Aplicação Eficaz da Lei

As opiniões expressas são apenas dos peritos e não devem ser consideradas representativas da posição oficial da Comissão Europeia.

Introdução

A União Europeia constitui um espaço de liberdade, segurança e justiça, no respeito dos direitos fundamentais e dos diferentes sistemas e tradições jurídicos dos Estados-Membros[3]. Envida esforços para garantir um elevado nível de segurança, através de medidas de prevenção e luta contra a criminalidade grave e organizada, incluindo o reforço da cooperação policial e judiciária transfronteiras[4], excluindo qualquer interferência com a segurança nacional, que continua a ser da competência exclusiva dos Estados-Membros. A fim de assegurar uma abordagem eficaz da luta contra a criminalidade e outros desafios relacionados com a manutenção de um elevado nível de segurança, as autoridades de aplicação da lei devem poder desempenhar as suas funções de forma eficaz e legal e no pleno respeito dos direitos fundamentais, a fim de prevenir, detetar e investigar infrações penais e assegurar a sua ação penal, servir a justiça no interesse geral e, em particular, no das vítimas, e salvaguardar a segurança pública.

3 *Tratado sobre o Funcionamento da União Europeia* (TFUE), artigo 67.º, n.º 1.
4 *Ibid.*, n.º 3.

Nos últimos anos, apesar da criação, transmissão e armazenamento de quantidades cada vez maiores de dados, o acesso aos dados para fins de aplicação da lei tornou-se um desafio fundamental para a realização de investigações e ações penais relativas a infrações penais e para a aplicação efetiva da lei. A UE estabeleceu regras sólidas para facilitar o acesso transfronteiras a provas eletrónicas («regras da UE em matéria de provas eletrónicas»)[5]. Contudo, a ausência de obrigações de conservação de dados afeta negativamente a eficácia das regras relativas às provas eletrónicas, uma vez que não existe qualquer garantia de que estejam disponíveis todas as informações sujeitas a ordens europeias de conservação ou de entrega de provas, incluindo dados de tráfego, dados solicitados com o único objetivo de identificar o utilizador e dados de assinantes. Além disso, as regras da UE em matéria de provas eletrónicas abrangem apenas os dados na posse de prestadores de serviços e não abordam o desafio da cifragem. Por conseguinte, sem medidas operacionais para o acesso lícito aos dados, corre-se o risco de não assegurar uma aplicação eficaz da lei. Para efeitos do presente documento, entende-se por «acesso aos dados» o acesso concedido às autoridades de aplicação da lei, sujeito a autorização judicial *ex ante*, quando necessário, para efeitos de investigações criminais e numa base casuística. Regra geral, nos casos em que essa autorização judicial é necessária devido à natureza sensível dos dados em causa, constitui parte integrante do quadro jurídico e operacional aplicável. O acesso aos dados deve ser obtido no pleno respeito dos direitos fundamentais, bem como da jurisprudência do Tribunal de Justiça da União Europeia (TJUE) e dos acórdãos do Tribunal Europeu dos Direitos do Homem sobre estas matérias, bem como das garantias processuais aplicáveis.

5 *Ver E-evidence – cross-border access to electronic evidence (Provas eletrónicas – acesso transfronteiras a provas eletrónicas) – Comissão Europeia (europa.eu). As novas regras entrarão em vigor em 17 de agosto de 2023 e serão aplicáveis a partir de 17 de fevereiro, no caso da diretiva, e 17 de agosto de 2026, no caso do regulamento.*

Este desafio está desde há muito na agenda política. Mais especificamente, o Conselho Europeu, o Conselho[6], o Parlamento Europeu[7], o TJUE e as agências da UE debateram e formularam conclusões, por diversas vezes, sobre vários aspetos jurídicos e políticos do acesso aos dados de comunicações eletrónicas, incluindo os dados de tráfego e de localização (metadados) e, de um modo mais geral, às provas eletrónicas. Já nas suas Conclusões de 22 e 23 de junho de 2017[8], o Conselho Europeu apelou a que se desse «resposta aos desafios colocados por sistemas que permitem aos terroristas comunicar por meios a que as autoridades competentes não podem ter acesso, incluindo a criptografia de ponta a ponta, salvaguardando porém os benefícios que estes sistemas proporcionam em matéria de proteção da privacidade, dos dados e das comunicações» e salientou que o «acesso efetivo a meios de prova eletrónicos é essencial na luta contra a criminalidade grave».

Na Estratégia da UE para lutar contra a criminalidade organizada (2021–2025) salienta-se a importância do acesso às comunicações eletrónicas para lutar contra a criminalidade organizada e para adaptar as autoridades de aplicação da lei e o sistema judiciário à era digital[9]. O acesso aos dados é também de importância fundamental em todas as prioridades da EMPACT na luta contra a criminalidade grave e organizada para 2022-2025[10], e na Estratégia da UE para a União da Segurança declara-se que a Comissão estudará medidas destinadas a reforçar a capacidade dos serviços repressivos nas investigações digitais[11]. Em 2023, a Presidência sueca do Conselho apresentou o documento «Law Enforcement – Operational Needs for Lawful Access to Communications» [Aplicação da lei – Necessidades operacionais para um acesso lícito às comunicações] (LEON[12]), que estabelece uma lista exaustiva das necessidades operacionais das autoridades de aplicação da lei no que diz respeito às redes e serviços de comunicações[13].

---

6 10007/16, *Conclusões do Conselho sobre a melhoria da justiça penal no ciberespaço.*

7 JO 2018/C 346/04, *Resolução do Parlamento Europeu, de 3 de outubro de 2017, sobre a luta contra a cibercriminalidade.*

8 EUCO 8/17.

9 *Comunicação da Comissão sobre a estratégia da UE para lutar contra a criminalidade organizada (2021-2025),* COM(2021)170, Bruxelas, 14 de abril de 2021.

10 8665/21.

11 *Comunicação da Comissão sobre a Estratégia da UE para a União da Segurança,* COM/2020/605, 24 de julho de 2020.

12 LEON é o resultado dos trabalhos realizados pelos serviços responsáveis pela aplicação da lei da Suécia, em estreita cooperação com os representantes dos serviços responsáveis pela aplicação da lei nos Estados-Membros da UE, na América do Norte e na Austrália. O objetivo é identificar e descrever as necessidades dos serviços responsáveis pela aplicação da lei para o acesso lícito ao conteúdo das comunicações, aos dados relacionados com o conteúdo e às informações dos assinantes.

13 *Comunicação da Presidência do Conselho sobre as necessidades operacionais dos serviços responsáveis pela aplicação da lei para o acesso lícito às comunicações (LEON),* 6050/23 de 16 de fevereiro de 2023.

A fim de identificar possíveis vias a seguir, a Presidência sueca, em cooperação com as subsequentes Presidências espanhola e belga, lançou, em junho de 2023, o grupo de peritos de alto nível sobre o acesso aos dados para uma aplicação eficaz da lei (GAN), composto por representantes de alto nível dos Estados-Membros, da Comissão, dos órgãos e organismos competentes da UE e do Coordenador da Luta Antiterrorista da UE[14]. Este grupo é copresidido pela Comissão e pela Presidência rotativa do Conselho da UE e estudou os desafios que os profissionais responsáveis pela aplicação da lei na União enfrentam no seu trabalho quotidiano em matéria de acesso aos dados, tendo identificado potenciais soluções e recomendações para os superar, com o objetivo de assegurar a disponibilidade de instrumentos eficazes de aplicação da lei para combater a criminalidade e reforçar a segurança pública na era digital, no pleno respeito dos direitos fundamentais.

Ao longo do seu trabalho, o GAN identificou amplas provas da falta de acesso efetivo aos dados e transmitiu repetidamente que essa falta de acesso é persistente, se não mesmo crescente. Além disso, estão ainda a ser recolhidas novas provas através de consultas específicas. Os dados de comunicação gerados, tratados ou armazenados digitalmente (metadados e dados de conteúdo) são uma componente importante das investigações criminais modernas[15]. Uma vez que os criminosos dependem cada vez mais de serviços em linha, os pedidos de dados aos prestadores de serviços em linha triplicaram entre 2017 e 2022[16].

---

14 *Decisão da Comissão que cria um grupo de peritos de alto nível sobre o acesso aos dados para uma aplicação eficaz da lei*, C(2023) 3647 de 6 de junho de 2023.

15 Avaliação de impacto que acompanha a proposta de regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal e a proposta de diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal, {COM(2018) 225 final} – {COM(2018) 226 final} – {SWD(2018) 119 final}.

16 Relatório SIRIUS 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, p. 69.

O GAN defende que as autoridades de aplicação da lei enfrentam desafios operacionais crescentes quando procuram aceder legalmente a dados gerados, tratados ou armazenados digitalmente num formato legível. Entre os inquiridos no âmbito do inquérito anual mais recente do projeto SIRIUS sobre o acesso transfronteiras a provas eletrónicas, 47 % identificaram a falta de conservação de dados como o principal desafio que enfrentaram[17] e, já em 2018, estimava-se que até 2019 mais de 22 % das mensagens mundiais fossem cifradas de ponta a ponta e inacessíveis às autoridades de aplicação da lei[18]. O GAN identificou a falta de um quadro jurídico adequado para a interceção legal de serviços de telecomunicações não tradicionais como tendo também consequências significativas para as medidas de aplicação da lei: mais de 90 % das mensagens passam por serviços sobrepostos.

Para fazer face a estes desafios, o GAN formulou recomendações estratégicas e prospetivas para dar resposta aos desafios atuais e previstos no contexto da evolução tecnológica, permitindo uma abordagem abrangente da UE que assegure o acesso aos dados para uma aplicação eficaz da lei. Estas recomendações foram formuladas pelos peritos dos grupos de trabalho do GAN, selecionados pelos Estados-Membros e pelos órgãos e organismos competentes da UE. Entre os peritos contam-se principalmente representantes das autoridades policiais e judiciárias, mas também profissionais da cibersegurança e peritos em proteção de dados.

As recomendações apresentadas de seguida no relatório foram formuladas no contexto dos três casos de utilização em torno dos quais os grupos de trabalho foram organizados. As recomendações foram agrupadas sob o fluxo de trabalho pertinente e aprovadas pelo GAN na sua 4.ª reunião plenária, em 21 de maio de 2024. Numa segunda fase, estas recomendações serão operacionalizadas e objeto de uma avaliação da viabilidade jurídica, técnica e financeira, tendo em conta os limitados recursos orçamentais e humanos disponíveis ao abrigo do orçamento da UE, com vista à apresentação de um relatório final no outono de 2024.

---

17 *Ibid*, p. 46.

18 https://www.csis.org/blogs/strategic-technologies-blog/scoping-law-enforcements-encrypted-messaging-problem.

Principais fatores subjacentes às recomendações

Os contributos supra, bem como os debates pormenorizados em três reuniões plenárias do GAN, nove reuniões de grupos de peritos, uma reunião de consulta pública e os contributos escritos, permitiram identificar os principais fatores problemáticos subjacentes aos desafios acima referidos e fundamentar as recomendações.

Relativamente ao **acesso aos dados inativos nos dispositivos dos utilizadores**, o GAN identificou as principais questões: ausência de cooperação transfronteiras em matéria de aplicação da lei no que toca à partilha de ferramentas de criminalística digital; cooperação insuficiente entre as autoridades de aplicação da lei e os fornecedores, fabricantes e distribuidores de *hardware* e *software* pertinentes, o que dificulta a capacidade de aceder aos dados não cifrados; dificuldade em aceder legalmente ao dispositivo de um utilizador e, quando o acesso é possível, em extrair e decifrar os dados e metadados disponíveis para obter informações inteligíveis que possam ser úteis para as investigações e apresentadas como elementos de prova admissíveis em tribunal.

O GAN considera que o ritmo dos desenvolvimentos tecnológicos relacionados com a **cifragem** das informações nos dispositivos é rápido, ao ponto de as ferramentas e técnicas de decifragem existentes se tornarem ineficazes, o que é especialmente verdade nos casos em que os suspeitos e os grupos de criminalidade organizada utilizam dispositivos e redes de comunicação concebidos especificamente. O tempo necessário para decifrar os dados extraídos dos dispositivos é também uma questão importante: os peritos indicaram que, em alguns casos, pode demorar até dois anos. O grau de dificuldade envolvido na decifragem de dispositivos personalizados concebidos e comercializados exclusivamente para fins criminosos é ainda mais elevado e coloca novos desafios aos serviços de criminalística digital em todos os Estados-Membros.

Não obstante, é importante que as soluções técnicas que permitem às autoridades utilizar os seus poderes de investigação preservem todas as vantagens da cifragem por motivos de proteção de dados, privacidade, cibersegurança e segurança nacional. Este princípio de «segurança através da cifragem e da segurança apesar da cifragem» foi um princípio central dos debates do GAN, e as futuras soluções técnicas ou ferramentas desenvolvidas não devem resultar no enfraquecimento ou comprometimento das tecnologias de encriptação para a comunicação de outros utilizadores que não estão sujeitos à medida de acesso lícito.

Uma questão fundamental levantada pelo GAN é a **falta de mecanismos de cooperação transfronteiras em matéria de aplicação da lei** no que diz respeito à partilha de ferramentas de criminalística digital entre os Estados-Membros, uma vez que estes têm frequentemente soluções distintas para problemas técnicos semelhantes. Apesar de a Europol alojar um repositório interno de ferramentas a que as autoridades de aplicação da lei nacionais podem aceder e delas fazer uso, é provável que os Estados-Membros tenham acesso a outras ferramentas e a *software* de decifragem personalizado. Contudo, abstêm-se de os partilhar, quer por falta de confiança e de comunicação entre os serviços de criminalística digital competentes, quer por não estarem autorizados a fazê-lo por lei, muitas vezes devido a preocupações de segurança nacional.

O GAN concordou que **redes**, como a Rede Europeia de Institutos de Polícia Científica (ENFSI)[19], dedicadas à coordenação e partilha de conhecimentos sobre métodos, ferramentas e boas práticas de criminalística digital são fundamentais para os profissionais de criminalística digital em toda a UE. Estas redes já existem, mas, para melhorar a comunicação e a colaboração entre os serviços de criminalística digital dos diferentes Estados-Membros, deverão continuar a ser apoiadas e identificadas para promover uma maior partilha de conhecimentos e ferramentas[20], com o apoio de um sistema centralizado. O GAN sublinhou igualmente que o custo das ferramentas de criminalística digital comerciais constituía um obstáculo significativo com que todos os Estados-Membros se deparavam e que se deveria reforçar a investigação e o desenvolvimento de ferramentas a nível da UE, bem como a utilização dos mecanismos já existentes, como a Associação Europeia de Desenvolvimento de Tecnologias Contra a Cibercriminalidade (EACTDA) e o repositório de ferramentas da Europol para a sua divulgação[21]. A avaliação e a certificação das ferramentas comercialmente disponíveis constituíram mais um ponto de debate recorrente[22] e o GAN concordou, de um modo geral, que era necessário um mecanismo ou sistema para assegurar que essas ferramentas cumprem as normas forenses e de responsabilização da União. A avaliação e a certificação são necessárias para garantir que as tecnologias cumprem os requisitos de fiabilidade (por exemplo, requisitos em matéria de integridade dos dados ao longo do processo de criminalística digital), independentemente de o fabricante estar estabelecido dentro ou fora da UE.

---

19 https://enfsi.eu/.
20 Ver recomendação 1.
21 Ver recomendações 3 e 4.
22 Ver recomendação 5.

Entre os problemas identificados pelo grupo de alto nível conta-se também a **diminuição da comunicação** entre as autoridades de aplicação da lei e os fornecedores de *hardware* e *software*; consequentemente, as autoridades de aplicação da lei deparam-se com dificuldades quanto à forma de colaborar com a indústria para que lhes seja concedido acesso aos dados nos dispositivos apreendidos. O GAN constatou que a falta de conhecimentos afeta as interações que as autoridades de aplicação da lei têm com os produtores de *hardware* e *software*. A diminuição da comunicação entre as autoridades de aplicação da lei e a indústria também levou ao estabelecimento de menos protocolos para o acesso lícito aos dados nos dispositivos dos utilizadores. O GAN determinou que a falta de participação das autoridades de aplicação da lei nos organismos de normalização afeta a possibilidade de moldar os protocolos dos produtos e a arquitetura técnica de modo a assegurar que as suas preocupações e requisitos técnicos sejam tidos em conta numa fase precoce do desenvolvimento de futuras normas tecnológicas[23].

Uma última questão fundamental abordada pelo GAN foi o facto de, na ausência de cooperação voluntária, a **ausência de obrigações no sentido de a indústria** cooperar com os pedidos das autoridades de aplicação da lei policiais de acesso aos dados inativos nos dispositivos dos utilizadores estar a afetar negativamente a sua capacidade de realizar investigações exaustivas. Constataram que não existe uma visão global das obrigações existentes a nível dos Estados-Membros[24].

No que diz respeito ao **acesso aos dados inativos nos sistemas dos prestadores de serviços**, a primeira questão fundamental que as autoridades de aplicação da lei enfrentam gira em torno das discrepâncias entre os quadros jurídicos nacionais que regulam a conservação de dados nos sistemas dos prestadores de serviços e a duração dessa conservação.

---

[23] Ver recomendação 12.

[24] Ver recomendação 25.

Os peritos salientaram, nomeadamente, a atual ausência de qualquer nível de **harmonização da legislação em matéria de conservação de dados** na UE e as dificuldades em cumprir os critérios indicados pelo TJUE, que limitam a conservação generalizada e indiscriminada de dados de tráfego e de dados de localização em circunstâncias específicas ao combate a ameaças graves para a segurança e que apenas permitem a conservação seletiva desses dados para combater a criminalidade grave. Em especial, o conceito de «conservação seletiva de dados» está a revelar-se muito difícil de aplicar pelos Estados-Membros, em parte também porque alguns dos critérios foram concebidos com base em tecnologias que evoluíram desde que os acórdãos foram proferidos[25], e persiste uma falta de clareza quanto aos tipos de dados que podem ser consultados no caso de infrações não graves.

O GAN considerou que uma abordagem harmonizada da conservação de dados a nível da UE é indispensável para investigações eficazes, em especial em processos transfronteiriços, e para a admissibilidade dos elementos de prova nos tribunais. O GAN debateu ainda a forma como a ausência de obrigatoriedade de conservação de dados pode afetar a eficácia das novas regras em matéria de provas eletrónicas, uma vez que os dados de tráfego sujeitos a ordens europeias de conservação ou de entrega de provas podem não estar disponíveis.

O GAN partilhou a opinião de que todas as soluções para os desafios atuais têm de ser tecnologicamente neutras, a fim de abranger quaisquer desenvolvimentos técnicos futuros. A tónica foi colocada na necessidade de tais soluções criarem obrigações para todos os prestadores de serviços, incluindo os serviços sobrepostos, que deverão ser forçados a responder aos pedidos das autoridades de aplicação da lei e a ser mais transparentes no que diz respeito aos dados que recolhem para fins empresariais. Esse regime poderia ser alcançado através de **legislação ou de medidas não vinculativas**, com preferência pelas primeiras[26].

---

25 Por exemplo, as tecnologias como os endereços IP dinâmicos e a tradução de endereços de rede de operador (*Carrier Grade Net Address Translation* – CGNAT) não estavam plenamente desenvolvidas aquando da publicação dos acórdãos do TJUE que sugeriram a conservação de dados com base na delimitação geográfica (como referência, consultar os processos Digital Rights Ireland, de 2014, e Tele2 Sverige AB, de 2016).

26 Ver recomendação 27.

À luz da jurisprudência em matéria de conservação de dados, o GAN debateu a aplicação prática da **conservação seletiva** e salientou as dificuldades encontradas na aplicação dos requisitos do Tribunal (ou seja, a conservação seletiva com base em critérios geográficos e categorias de pessoas). A aplicação dos requisitos do Tribunal foi considerada problemática pelos peritos no que diz respeito aos direitos fundamentais (devido à discriminação contra categorias de pessoas ou à localização), de um ponto de vista operacional, uma vez que o direcionamento da recolha de dados reduz drasticamente a capacidade de acesso a informações essenciais para as investigações e, do ponto de vista da execução técnica, para os operadores. À luz destas considerações, muitos peritos afirmaram que o regime da UE deveria centrar-se não só na conservação, mas também no acesso. Em especial, alguns peritos expressaram a opinião de que a diferenciação dos prazos de acesso aos dados conservados com base em categorias de criminalidade deveria ser o único critério a regular os regimes de conservação de dados e que as soluções para um acesso muito direcionado devem ser concebidas com base noutros critérios[27]. Contudo, outros peritos manifestaram a sua preocupação quanto à conformidade destas medidas com a jurisprudência do TJUE, uma vez que a jurisprudência do TJUE se aplica tanto à conservação como ao acesso aos dados.

Entre os problemas identificados, as autoridades de aplicação da lei também enfrentam dificuldades relacionadas com os **tipos de metadados conservados** pelos prestadores de serviços. Sempre que existem obrigações legais, por vezes estas são flexíveis no que diz respeito aos tipos de metadados que os prestadores de serviços de comunicações devem conservar, o que resulta numa variedade de dados disponíveis, com diferentes graus de utilidade como pistas de investigação. O GAN é da opinião de que a UE deveria exigir que fossem impostos níveis mínimos de conservação aos operadores a nível da UE (no mínimo, os dados necessários para identificar o utilizador)[28]. O GAN concordou também que os prestadores de serviços que oferecem serviços cifrados devem ser obrigados a encontrar os meios para fornecer dados de forma inteligível, mediante pedido legal das autoridades judiciárias e de aplicação da lei[29].

---

27 Ver recomendação 29.
28 Ver recomendação 27.v.
29 Ver recomendação 27.iii.

A transição de fornecedores de comunicações tradicionais para a utilização de **serviços sobrepostos** é uma das principais causas das dificuldades que as autoridades de aplicação da lei enfrentam quando tentam aceder aos dados armazenados nos sistemas dos prestadores de serviços. Embora os serviços sobrepostos estejam abrangidos pelo âmbito de aplicação do Código Europeu das Comunicações Eletrónicas, não estão sujeitos a sistemas de licenciamento comparáveis que possam implicar obrigações. Os peritos debateram a necessidade imperiosa de regras que obriguem os serviços sobrepostos a conservar os dados também no caso de estarem sediados em jurisdições diferentes. A ausência de tais regras resulta numa falta de clareza e de segurança jurídica, que leva ao incumprimento por parte dos serviços sobrepostos. Além disso, por vezes, alguns serviços sobrepostos não conservam quaisquer dados.

O GAN concordou com a necessidade de **transparência** em relação aos dados gerados, tratados e armazenados pelos fornecedores de comunicações, incluindo, em especial, os serviços sobrepostos e outros serviços que oferecem «serviços de comunicação» (como os fabricantes de automóveis[30]), e debateu instrumentos que assegurem a conformidade antes de entrar em funcionamento no mercado da UE[31]. Os peritos debateram a oportunidade de legislar sobre os dados já na posse dos prestadores de serviços para fins comerciais[32].

Neste contexto, os peritos concordaram com a necessidade de estabelecer **mecanismos de cooperação** com o setor privado com vista a aumentar a transparência e sugeriram várias possibilidades de o fazer, nomeadamente através de memorandos de entendimento[33] e do reforço e da exploração plena das estruturas existentes, como o SIRIUS, a RJE[34] e/ou a RJEC[35].

---

30 Ver recomendação 17.
31 Ver recomendação 30.
32 Ver recomendação 31.
33 Ver recomendação 14.
34 A Rede Judiciária Europeia (RJE) em matéria penal é uma rede de pontos de contacto nacionais para facilitar a cooperação judiciária em matéria penal.
35 Ver recomendação 13.

O GAN considerou útil uma cooperação reforçada, nomeadamente no que diz respeito à definição de formatos normalizados para a conservação de dados[36]. Com efeito, embora exista uma norma desenvolvida sob os auspícios do Instituto Europeu de Normalização das Telecomunicações (ETSI) para os metadados das telecomunicações tradicionais, esta não é universalmente aplicada em todos os Estados-Membros, nem mesmo com os fornecedores de telecomunicações, e não existe acordo sobre um formato normalizado para a transmissão de dados dos serviços sobrepostos às autoridades de aplicação da lei, o que aumenta a complexidade da análise dos dados nos casos em que os dados podem ser fornecidos.

A **normalização** deverá ser prosseguida para assegurar uma categorização harmonizada dos dados a conservar e a aceder, mas também para estabelecer canais seguros para o intercâmbio entre as autoridades competentes e os prestadores de serviços. O GAN debateu várias possibilidades de o fazer, centrando-se, em especial, no reforço da participação coordenada dos representantes das autoridades de aplicação da lei nos organismos de normalização pertinentes[37].

A maioria dos Estados-Membros dispõe de quadros regulamentares nacionais específicos para o **acesso em tempo real aos dados de comunicação**, o que continua a ser um instrumento essencial para a luta contra a criminalidade, incluindo a criminalidade em linha e a criminalidade organizada, bem como o terrorismo.

No entanto, quando se trata de prestadores de serviços não tradicionais, as autoridades de aplicação da lei não podem depender de um quadro vinculativo e harmonizado. Com efeito, embora alguns Estados-Membros tenham estabelecido regulamentos que obrigam os serviços sobrepostos a responder aos pedidos lícitos de acesso, existe uma **aplicação desigual** entre os prestadores de serviços de comunicação e os serviços sobrepostos no acesso em tempo real aos dados, sendo que os serviços sobrepostos geralmente não cumprem essas obrigações por razões de ordem jurídica e técnica.

---

36 Ver recomendações 15 e 16.

37 Ver recomendação 20.

Os peritos concordaram que um dos principais objetivos seria **criar condições de concorrência equitativas entre os prestadores de serviços de comunicação[38] e outros tipos de fornecedores de comunicações eletrónicas** no que diz respeito às obrigações executórias de interceção legal; a interceção legal deve estar prevista na lei e ser autorizada por tribunais ou autoridades administrativas independentes, em conformidade com as normas técnicas e em plena conformidade com a proteção de dados e a privacidade, bem como com as medidas de cibersegurança e interoperabilidade. Os peritos esclareceram que, em muitos casos, a interceção legal de serviços de comunicações eletrónicas deverá ser a medida preferida de acesso aos dados em tempo real. Essas regras de interceção legal deverão basear-se em princípios que se aplicam atualmente aos fornecedores de comunicações tradicionais, por exemplo, em termos de supervisão e cooperação com os operadores de comunicações, mas também em termos de capacidade de acesso aos dados não cifrados quando as autoridades judiciais o considerem necessário e proporcionado[39].

As **diferenças entre os quadros jurídicos nacionais** dos Estados-Membros da UE em matéria de interceção de metadados ou de dados de conteúdo criam desafios para a aplicação da lei nos casos com elementos transfronteiriços. Por exemplo, pode ser difícil para as autoridades de aplicação da lei intercetar comunicações em tempo real entre dois cidadãos do seu país que utilizam um serviço de comunicação alojado noutro Estado-Membro da UE com diferentes requisitos processuais para a interceção em direto. Os peritos debateram a oportunidade de resolver estas questões a nível da UE, especificando as diferentes medidas que poderiam ser aplicadas para o efeito, por exemplo, ações legislativas[40]. A insegurança jurídica decorrente dos diferentes requisitos dos quadros jurídicos nacionais em matéria de interceção foi um tema central do debate entre os peritos, que se debruçaram sobre a necessidade de abordar questões como a aplicação territorial de determinadas obrigações, o que resulta em conflitos de leis e atrasos ou obstáculos administrativos às investigações[41].

Além das questões determinadas pela falta de legislação harmonizada em todos os Estados-Membros, os peritos debateram também o facto de **a falta de conhecimento da localização exata dos utilizadores e dos dados aumentar frequentemente a complexidade da determinação do nexo territorial de uma infração penal**.

---

38 Fornecedores de telecomunicações tradicionais de acordo com a definição do ETSI, ou seja, proprietários de infraestruturas.

39 Ver recomendação 37.

40 Ver recomendação 38.

41 Ver recomendação 39.

Os peritos acordaram simultaneamente em continuar a aplicar a decisão europeia de investigação (DEI) como instrumento para solicitar a interceção por outro Estado-Membro e para o intercâmbio de elementos de prova recolhidos através da interceção, e debateram também os seus limites, incluindo os relacionados com a aplicabilidade parcial em todos os Estados-Membros[42].

O conceito de «competência territorial» em matéria de dados foi abordado durante os debates. Os peritos consideraram que, nos casos em que o nexo seja nacional (por exemplo, um crime cometido num Estado-Membro por um criminoso que se situa no mesmo Estado-Membro), a autoridade do Estado-Membro deverá poder adotar medidas de interceção, em conformidade com o direito processual nacional que estabeleça requisitos e garantias, sem ter de recorrer a um instrumento de cooperação transfronteiriça. Quando necessário a fim de ultrapassar os conflitos de direito com outras jurisdições, os peritos debateram possíveis iniciativas que a UE poderia tomar, inspirando-se no Regulamento Provas Eletrónicas, e que consistem também em acordos bilaterais com países como os Estados Unidos, apoiados por uma análise mais aprofundada e por uma avaliação de impacto que tenha igualmente em conta os direitos fundamentais e a soberania do Estado.

Os peritos partilharam a opinião de que se poderia procurar um certo nível de harmonização a nível da UE através de instrumentos jurídicos não vinculativos (por exemplo, uma recomendação da Comissão), e sugeriram simultaneamente que as necessidades operacionais comuns da LI poderiam ser desenvolvidas com base no documento LEON[43].

Do ponto de vista técnico, os peritos debateram **a necessidade de criar mecanismos e infraestruturas compatíveis com a transferência em tempo real de quantidades potencialmente muito elevadas de dados de natureza diversa intercetados**[44]. A este respeito, os peritos debateram exaustivamente os benefícios da normalização e as possíveis abordagens neste domínio. Apelaram a uma representação mais forte dos governos/administrações nacionais no desenvolvimento de normas para as redes 5G/6G e para as comunicações em geral, insistindo na necessidade de estar presente nas instâncias mais relevantes, como o 3GPP, o ETSI, a ISO e a UIT. Também consideram que é necessário o apoio da Comissão, da Europol ou de outros órgãos e organismos da UE[45].

---

42 Ver recomendação 40.
43 Ver recomendação 21.
44 Ver recomendação 9.
45 Ver recomendação 20.

Paralelamente, os peritos debateram aprofundadamente os casos relativos a prestadores não cooperantes para que seja possível aplicar-lhes as sanções administrativas e/ou penais, conforme o grau de negligência, adequadas[46]. Os peritos concordaram que qualquer futuro instrumento da UE a este respeito deverá ter em conta esta diferença[47]. Deverá também ter em conta o acervo da UE, nomeadamente o Regulamento Serviços Digitais.

Nos casos de prestadores não cooperantes, os peritos debateram e partilharam a opinião de que, independentemente dos instrumentos jurídicos em vigor, em **casos específicos** (no caso, sobretudo, dos serviços criminosos, como o EncroChat), as **autoridades de aplicação da lei continuarão a ter de recorrer à utilização de vulnerabilidades** (ou seja, medidas intrusivas). Embora se tenha chegado a consenso quanto ao facto de esses casos deverem continuar a ser excecionais e de essas soluções estarem longe de ser ideais, é importante cooperar no que toca à harmonização destes aspetos, especialmente tendo em conta o estabelecimento de salvaguardas[48] e, possivelmente, de regras harmonizadas para a admissibilidade mútua dos elementos de prova entre os Estados-Membros, na medida do necessário para facilitar o reconhecimento mútuo das sentenças, decisões judiciais e cooperação policial e judiciária em matéria penal[49]. Os peritos salientaram a forma como as operações conduzidas pelas autoridades contra a EncroChat ou a Sky ECC são contestadas nos tribunais e salientaram a incerteza jurídica resultante dos diferentes requisitos das legislações nacionais no que diz respeito à utilização de um resultado de uma interceção num Estado-Membro como elemento de prova noutro.

Outra questão identificada como problema e amplamente debatida diz respeito ao **acesso aos dados em formato legível**.

Para além dos problemas de acesso aos dados nos dispositivos, a cifragem acrescenta um nível de complexidade quando se trata do acesso a dados de conteúdo em tempo real, tanto para os serviços sobrepostos, quando aplicam um mecanismo de cifragem de ponta a ponta, como para os operadores de telecomunicações tradicionais quando, por exemplo, implementam o «encaminhamento para a rede local» para as redes 5G.

---

46 Ver recomendação 33.
47 Ver recomendação 34.
48 Ver recomendação 10.
49 Ver recomendação 42.

No que diz respeito ao **acesso aos dados de conteúdo apesar da cifragem**, os peritos procederam a um debate exaustivo e concordaram com a necessidade de as autoridades de aplicação da lei terem acesso aos dados não cifrados. Salientaram que as soluções tecnológicas podem ser aplicadas sempre que existam ou deverão ser desenvolvidas para preservar a privacidade e a proteção de dados, garantir a cibersegurança e permitir a aplicação simultânea de medidas específicas de acesso lícito, nomeadamente em matéria de dados de conteúdo. Os peritos debateram a necessidade de normalização para dar resposta aos requisitos operacionais da aplicação da lei, nomeadamente em novas normas de telecomunicações, como a tecnologia 6G. Deverão ser desenvolvidas normas que permitam um acesso lícito sem enfraquecer a privacidade, a proteção de dados e os mecanismos de cibersegurança[50] para as tecnologias da comunicação presentes e futuras. Esta abordagem, que implica a avaliação e certificação de sistemas de interceção legal para garantir que os requisitos de cibersegurança, privacidade e acesso lícito são efetivamente cumpridos, abre uma perspetiva a mais longo prazo, inclusive no que respeita a tecnologias futuras, como a tecnologia 6G.

Os peritos manifestaram o desejo de **começar por explorar os aspetos técnicos**, em coordenação com peritos em cibersegurança. Os peritos clarificaram a necessidade de dar resposta aos desafios da cifragem (e, de um modo mais geral, da interceção em tempo real) **a partir da conceção das tecnologias da comunicação**, nomeadamente através do **desenvolvimento de projetos que envolvam peritos em tecnologia, cibersegurança, privacidade, normalização e segurança**. Salientaram que, para desempenharem as suas funções no mundo digital, as autoridades de aplicação da lei precisam de ter um acesso lícito preestabelecido a dados legíveis, em conformidade com instrumentos internacionais, como a Convenção de Budapeste, preservando simultaneamente os requisitos de cibersegurança. Para o efeito, o GAN apelou à UE para que estabelecesse um roteiro e coordenasse o trabalho através de um processo de estrutura permanente, possivelmente organizado pelo Polo da UE de Inovação para a Segurança Interna[51].

[50] Ver recomendação 23.
[51] Ver recomendação 22.

No que diz respeito ao que precede, outros elementos preocupantes incluíram a utilização de serviços de comunicações enriquecidas para o intercâmbio de SMS de uma forma cifrada de ponta a ponta, o aumento da comunicação 5G para assinantes itinerantes de entrada e iniciativas como a Apple Private Relay. Tecnologias como estas retiraram aos prestadores de serviços de telecomunicações tradicionais as informações mais pertinentes, de outro modo disponíveis sem cifragem, afetando assim a capacidade das autoridades de aplicação da lei de acederem a dados em trânsito em tempo real, de forma eficaz e legal. Os peritos debateram estes desafios e salientaram a necessidade de manter as capacidades de interceção legal no caso dos operadores de telecomunicações tradicionais, não obstante as redes 5G e 6G, e apelaram a que a cooperação com os prestadores de serviços fosse facilitada a nível da UE[52].

[52] Ver recomendação 24.

Recomendações do Grupo de Alto Nível

No que respeita às medidas de reforço de capacidades, o Grupo de Alto Nível recomenda:

1. Proceder ao levantamento das **redes de criminalística digital existentes** e estabelecer ligação entre as mesmas, aumentando simultaneamente a acessibilidade, evitando sobreposições e promovendo a liderança. No que diz respeito ao último aspeto, deverá ser criado um secretariado para as redes, a fim de simplificar a divulgação de conhecimentos entre peritos; o secretariado deverá refletir sobre mecanismos para assegurar que as ferramentas sensíveis possam ser partilhados no pleno respeito das regras nacionais.

2. Refletir sobre **mecanismos de partilha de conhecimentos**, a fim de assegurar que as ferramentas de criminalística digital possam ser partilhadas entre os Estados-Membros num ambiente de confiança, tendo simultaneamente em conta as regras nacionais. Tal poderá incluir a análise de uma abordagem europeia para a gestão e divulgação das vulnerabilidades tratadas pelas autoridades de aplicação da lei, com base nas boas práticas existentes.

3. O desenvolvimento de um mecanismo a nível da UE para a **aquisição conjunta de licenças de ferramentas de criminalística digital**, a fim de as partilhar entre os Estados-Membros.

4. Aumentar o **financiamento para a investigação e o desenvolvimento de ferramentas para a recolha de dados, o acesso a dados não cifrados, incluindo capacidades de decifragem, e capacidades de análise de dados baseadas na inteligência artificial** com resultados concretos claros, e promover o repositório de ferramentas da Europol como plataforma central para a divulgação destas ferramentas.

5. Criar um **mecanismo/sistema para a avaliação e – quando pertinente – para a certificação de ferramentas de criminalística digital comerciais** a nível da UE, estando ciente de qualquer impacto potencialmente negativo nos processos de investigação e ação penal (como a imposição de encargos desnecessários).

6. Criar um processo dedicado ao **intercâmbio de capacidades** que possam implicar a utilização de vulnerabilidades, o que permitiria a partilha de conhecimentos e de recursos, respeitando simultaneamente a confidencialidade e a sensibilidade das informações.

7. Aumentar o número de **oportunidades de formação** para peritos e criar um **sistema de certificação a nível da UE para peritos em criminalística digital** (incluindo os que trabalham na decifragem), a fim de garantir a qualidade e a uniformidade da formação técnica ministrada.

8. Realizar investimentos para colmatar o défice de competências técnicas em matéria de normalização e para aumentar a sensibilização através da celebração de **acordos com o meio académico** e com outros institutos competentes.

9. Criar **mecanismos (interoperabilidade e cibersegurança) e infraestruturas (largura de banda e escalabilidade) que sejam compatíveis com a transferência em tempo real de grandes conjuntos de dados**, como os recolhidos quando as autoridades de um Estado-Membro executam um pedido de acesso lícito em nome de outro Estado-Membro. Tal implica a prossecução dos trabalhos relativos à normalização das estruturas de dados, aos mecanismos de confiança e à filtragem de dados, a fim de evitar a transmissão de dados que não sejam relevantes para a(s) investigação(ões) e cumprir os princípios em matéria de proteção de dados, incluindo a limitação da finalidade, a proporcionalidade e a minimização dos dados, a par do trabalho realizado a nível da UE sobre a conceção e o dimensionamento dos meios de transmissão e os custos associados.

10. Trabalhar, de forma mais coordenada e com o apoio do financiamento da UE, numa **metodologia destinada a desenvolver, tratar e utilizar medidas específicas de acesso lícito** para dar resposta a casos em que o acesso aos dados não seja possível através da cooperação com os serviços de comunicações eletrónicas. Tendo em conta a natureza sensível desta abordagem, a mesma deverá estar sujeita a autorização judicial e dispor de um quadro sólido em matéria de admissibilidade das provas. Esses casos deverão continuar a ser excecionais – ou seja, as autoridades de aplicação da lei só deverão utilizar esses instrumentos como medida de último recurso – e ser sujeitos a avaliações obrigatórias da proporcionalidade.

No que respeita à cooperação com a indústria e à normalização, o Grupo de Alto Nível recomenda:

11. A criação de uma **plataforma (equivalente ao SIRIUS[53])** para partilhar ferramentas, boas práticas e conhecimentos sobre a forma de obter acesso aos dados dos proprietários e produtores de produtos. Tendo como base o SIRIUS, essa plataforma deverá ser ampliada de modo a incluir no seu mandato os fabricantes de *hardware* e a criar pontos de contacto para efeitos de aplicação da lei com fabricantes de *hardware* e *software* digitais, e a fazer um levantamento desses pontos de contacto.

12. Promover a **cooperação com produtores e criadores de ferramentas de criminalística digital** a fim de simplificar a estrutura e o formato dos dados obtidos pelas autoridades de aplicação da lei através da utilização dessas ferramentas, preferencialmente seguindo as normas acordadas.

13. Continuar a financiar, expandir e **criar, a título permanente, estruturas e instâncias da UE**, incluindo o SIRIUS, a RJE e/ou a RJEC, com o objetivo de: a) desenvolver os contactos entre profissionais e prestadores de serviços para apoiar o intercâmbio de informações, o reforço de capacidades e a formação, b) fomentar um diálogo permanente, inclusive através de um fórum ou de uma autoridade independente que reúna profissionais (autoridades de aplicação da lei, magistrados e prestadores de serviços), a fim de definir os princípios e as modalidades de cooperação. Tal poderá incluir a criação ou o apoio à criação de um **repositório central de instrumentos e informações** (CRIP) que permita a partilha de jurisprudência, alterações da legislação e outras informações que sejam pertinentes para os Estados-Membros e os prestadores de serviços.

---

53 O SIRIUS é um projeto financiado pela UE que ajuda as autoridades judiciárias e de aplicação da lei a aceder a provas eletrónicas transfronteiras no contexto de investigações e processos penais. Operacionalizado em conjunto pela Europol e pela Eurojust, em estreita parceria com a Rede Judiciária Europeia, o projeto SIRIUS é um ponto de referência central na UE para a partilha de conhecimentos sobre o acesso transfronteiras a provas eletrónicas. O projeto SIRIUS ajuda os investigadores a lidar com a complexidade e com o volume de informação num ambiente em linha em rápida evolução. O projeto fornece produtos como orientações normalizadas sobre os processos de cooperação entre as autoridades competentes e os prestadores de serviços específicos. O SIRIUS presta outros serviços, como instrumentos de investigação e dados de contacto relativos aos prestadores de serviços, para além de facilitar oportunidades de partilha de experiências com os pares, tanto em linha como presencialmente.

14. A adoção, pelos Estados-Membros, de **memorandos de entendimento** enquanto mecanismo eficaz para promover a cooperação e desenvolver um entendimento comum entre os prestadores de serviços, o governo e os serviços responsáveis pela aplicação da lei, a fim de apoiar o aplicação da legislação nacional, recorrendo às melhores práticas estabelecidas em certos Estados-Membros.

15. O desenvolvimento de formatos de dados de acordo com as **normas elaboradas pelo Instituto Europeu de Normalização das Telecomunicações (ETSI)** ou por outros organismos de normalização, a fim de promover a interoperabilidade e facilitar a utilização por todos os Estados-Membros.

16. Substituir progressivamente os formatos específicos utilizados por cada prestador de serviços (e, consequentemente, pelas autoridades dos Estados-Membros) por uma abordagem horizontal, baseada em normas elaboradas pelo ETSI ou por outros organismos de normalização no que respeita ao formato dos pedidos e das respostas. *[A coerência da presente recomendação com as regras estabelecidas no Regulamento Provas Eletrónicas deverá ser objeto de uma avaliação mais aprofundada]*

17. **Promover regras de transparência aplicáveis aos prestadores de serviços de comunicações eletrónicas** no que diz respeito aos dados por eles tratados, gerados ou armazenados (uma vez que nem sempre coincidem) no decurso da sua atividade, e às informações a fornecer às autoridades de aplicação da lei sobre os dados disponíveis, tendo em conta os limites impostos pela confidencialidade das investigações. Os peritos sugerem que esse objetivo seja alcançado através de um acordo de cooperação com os prestadores de serviços ou, se necessário, do estabelecimento de obrigações vinculativas. É igualmente necessária uma maior transparência na aplicação das obrigações de interceção legal para fins judiciais, tanto por parte dos serviços de comunicações eletrónicas como por parte das autoridades. Essas regras deverão estar em consonância com o conceito de «segredo de investigação». Por exemplo, em todas as investigações, é imperativo que os suspeitos não sejam notificados durante todo o período em que decorre a investigação.

18. Criar um **centro coordenador** para identificar o(s) prestador(es) de serviços pertinente(s) e direcionar os pedidos lícitos que lhes sejam dirigidos (por exemplo, no que se refere à portabilidade dos números entre prestadores de serviços de telecomunicações, como já existe em alguns Estados-Membros da UE).

19. Estabelecer mecanismos para assegurar que os pedidos transfronteiriços sejam dirigidos aos prestadores de serviços de uma forma eficiente e que evite potenciais conflitos, inspirando-se nos mecanismos estabelecidos em relação às provas eletrónicas. *[A coerência da presente recomendação com as regras estabelecidas no Regulamento Provas Eletrónicas deverá ser objeto de uma avaliação mais aprofundada]*

20. Acompanhar as futuras iniciativas com **medidas de normalização** pertinentes. Para o efeito, sugere-se que a Comissão apresente um **roteiro** que inclua uma perspetiva a longo prazo, defina objetivos claros, preveja um financiamento adequado para apoiar uma maior participação de peritos dos Estados-Membros e proponha um mecanismo de coordenação, eventualmente através da Europol e de outras agências da UE. Importa assegurar que o âmbito das atividades de normalização seja amplo e abranja a Internet das coisas, incluindo os automóveis conectados, bem como quaisquer formas de conectividade, por exemplo, as comunicações por satélite. Deverão ser abrangidas as atividades relacionadas com a criminalística digital, o acesso lícito e a interceção legal.

21. Procurar inspiração para futuras iniciativas legislativas, práticas e técnicas numa **definição comum de requisitos**, como os estabelecidos no documento **LEON [*Law enforcement Operational Needs for Lawful Access to Communication* (Aplicação da lei – Necessidades operacionais para um acesso lícito às comunicações[54])]**. A criação de um grupo *ad hoc* de peritos, eventualmente coordenado pela Europol, assegurará que o documento LEON seja atualizado sempre que necessário, possivelmente sob a coordenação do grupo de trabalho sobre normalização para a segurança, gerido pela Europol, que deverá ser prosseguido. Todas as iniciativas deverão ser tecnologicamente neutras. Podem ser previstas diferentes opções a fim de remeter para o documento LEON em futuras iniciativas da UE: 1) proposta legislativa da UE que faça referência ao documento LEON, 2) recomendação e 3) fonte de inspiração.

[54] LEON é o resultado dos trabalhos realizados pelos serviços responsáveis pela aplicação da lei da Suécia, em estreita cooperação com os representantes dos serviços responsáveis pela aplicação da lei nos Estados-Membros da UE, na América do Norte e na Austrália. O objetivo é identificar e descrever as necessidades das autoridades de aplicação da lei para o acesso lícito ao conteúdo das comunicações, aos dados relacionados com o conteúdo e às informações dos assinantes.

22. Elaborar um roteiro tecnológico que reúna peritos em tecnologia, cibersegurança, privacidade, normalização e segurança e que garanta uma coordenação adequada, por exemplo, através de uma estrutura permanente, a fim de implementar o **acesso lícito desde a conceção** em todas as tecnologias pertinentes, em consonância com as necessidades expressas pelas autoridades de aplicação da lei, garantindo, ao mesmo tempo, uma segurança e cibersegurança sólidas e prevendo o pleno respeito das obrigações jurídicas em matéria de acesso lícito. De acordo com o GAN, as autoridades de aplicação da lei deverão contribuir para a definição de requisitos, mas não lhes deverá caber impor soluções específicas às empresas para que estas possam proporcionar um acesso lícito aos dados para fins de investigação criminal sem comprometer a segurança.

23. Garantir que eventuais novas obrigações, um novo instrumento jurídico e/ou normas **não conduzam, direta ou indiretamente, à obrigação de os fornecedores fragilizarem a segurança das comunicações**, comprometendo ou enfraquecendo, de um modo geral, a cifragem de ponta a ponta (E2EE). Por conseguinte, eventuais novas regras em matéria de acesso aos dados não cifrados teriam de ser submetidas a uma avaliação prudente com base em soluções tecnológicas de ponta (que, por sua vez, deverão ter em conta os desafios da cifragem). Ao garantirem a possibilidade de acesso lícito desde a conceção, conforme previsto por lei, os fabricantes ou os prestadores de serviços deverão fazê-lo de forma a que tal não tenha qualquer impacto negativo na postura de segurança das suas arquiteturas de *hardware* ou *software*.

24. Reforçar a **coordenação e o apoio da UE** para dar resposta a situações em que as soluções técnicas que permitem a interceção legal já existem, mas não são aplicadas pelos prestadores de serviços de comunicações eletrónicas. Nesses casos, por exemplo, quando os acordos de encaminhamento para a rede local ou a implementação específica do sistema de comunicações enriquecidas (RCS) não permitem capacidades de interceção lícitas, uma orientação clara e um diálogo facilitado a nível da UE melhorariam a cooperação com os serviços de comunicações eletrónicas.

No que respeita às medidas legislativas, o Grupo de Alto Nível recomenda:

25. Proceder a um **levantamento exaustivo** da legislação em vigor nos Estados-Membros, a fim de especificar as responsabilidades jurídicas dos fabricantes de *hardware* e *software* digitais no sentido de cumprirem os pedidos de dados por parte das autoridades de aplicação da lei. Tal teria igualmente em conta cenários e requisitos específicos que obrigam as empresas a aceder a dispositivos, em conformidade também com a jurisprudência do TJUE e a jurisprudência do Tribunal Europeu dos Direitos Humanos. O objetivo deverá consistir em, nessa base, elaborar um **manual a nível da UE** e, em função do levantamento acima referido, promover a aproximação da legislação neste domínio, e desenvolver normas vinculativas no setor aplicáveis aos dispositivos colocados no mercado na UE, a fim de integrar o acesso lícito.

26. Criar um **grupo de investigação para avaliar a viabilidade técnica de obrigações em matéria de acesso lícito incorporadas** (inclusive no que se refere ao acesso a dados cifrados) aplicáveis aos dispositivos digitais, mantendo e salvaguardando a segurança dos dispositivos e a privacidade das informações para todos os utilizadores, sem enfraquecer nem comprometer a segurança das comunicações.

27. Estabelecer um **regime harmonizado da UE em matéria de conservação de dados**, que tenha as seguintes características:

    i. tecnologicamente neutro e orientado para o futuro,

    ii. abrange os atuais e futuros «responsáveis pelo tratamento de dados» (ou seja, serviços sobrepostos e prestadores de serviços de qualquer tipo que possam conceder acesso a provas eletrónicas),

    iii. assegura o acesso a dados inteligíveis (no caso de metadados e dados de assinantes, o prestador de serviços deverá dispor de um meio para decifrar os dados, caso estes se encontrem cifrados, a qualquer momento durante a prestação do serviço),

    iv. centra-se não só na conservação de dados, mas também no acesso aos dados, com base nas regras relativas às provas eletrónicas,

    v. estabelece, no mínimo, a obrigação de as empresas conservarem dados suficientes para garantir que qualquer utilizador possa ser claramente identificado (por exemplo, endereço IP e número da porta);

    vi. plenamente conforme com as regras em matéria de proteção de dados e privacidade.

28. **Categorizar** os dados com base na sua finalidade (identificação, localização, determinação da atividade em linha de um titular de interesse), embora seja necessário algum trabalho para traduzir as finalidades em requisitos técnicos claros.

29. **Assegurar que o acesso aos dados é direcionado e diferenciado** em função das categorias de dados ou de categorias específicas de crimes (por exemplo, crimes que ocorrem apenas na Internet) ou com base na ameaça para as vítimas.

30. **Incluir regras em matéria de responsabilização e executoriedade** aplicáveis aos prestadores de serviços, a fim de fazer cumprir as obrigações de conservação e fornecimento de dados, por exemplo, através da aplicação de sanções administrativas ou de limites à operação no mercado da UE.

31. **Assegurar que os dados dos utilizadores conservados para fins comerciais e empresariais** são efetivamente acessíveis para efeitos de aplicação da lei ao abrigo das salvaguardas pertinentes.

32. Ponderar a possibilidade de **impor aos prestadores de serviços a obrigação** de ligarem ou desligarem determinadas funções nos seus serviços para obterem determinadas informações após receção de um mandado (por exemplo, armazenar a geolocalização de um utilizador específico depois de o mesmo ser visado por um pedido lícito).

33. Criar um mecanismo que garanta que os Estados-Membros possam **aplicar sanções** contra **serviços de comunicações eletrónicas não cooperantes**[55], e que essas medidas tenham um efeito dissuasor contra essas entidades. Deverão estar disponíveis tanto medidas administrativas como medidas de direito penal, que deverão ser aplicadas em função do facto de o prestador ser meramente não cooperante ou estar a acolher deliberadamente atividades de natureza criminosa.

34. Harmonizar, a nível da UE, as medidas de direito penal destinadas a garantir a cooperação, incluindo penas de prisão. O mesmo deverá aplicar-se aos **prestadores de serviços de alojamento virtual não cooperantes** (para além dos serviços de comunicações eletrónicas), a fim de assegurar que essas empresas, ao alojarem serviços de comunicações de natureza criminosa, cumpram devidamente as decisões judiciais que recebem. *[A coerência da presente recomendação com as regras estabelecidas no Regulamento Serviços Digitais deverá ser objeto de uma avaliação mais aprofundada]*

---

[55] Neste contexto, entende-se por **«serviços de comunicações eletrónicas não cooperantes»** qualquer operador que não cumpra as ordens legais e os pedidos de natureza técnica tratados pelas autoridades de aplicação da lei, e que não tenha qualquer razão objetiva para o fazer.

35. As potenciais iniciativas deverão efetuar uma distinção entre prestadores de **serviços de comunicações eletrónicas criminosos** (ou seja, plataformas especificamente concebidas para prestar serviços exclusiva ou principalmente a agentes criminosos, como a EncroChat) e **serviços de comunicações eletrónicas não cooperantes**, que estão legalmente estabelecidos e realizam atividades lícitas, mas que não cumprem plenamente as obrigações nacionais em matéria de interceção legal.

36. Estabelecer uma **obrigação vinculativa para as plataformas** (ou, em alternativa, medidas não vinculativas através da cooperação com o setor) no sentido de designarem um **SPOC**[56] **(ponto único de contacto)** na UE para o tratamento dos pedidos e dos contactos das autoridades da UE, especialmente no caso de prestadores de serviços para os quais é necessário um contacto de emergência. Deverá também existir um mecanismo semelhante (ou, idealmente, o mesmo SPOC, com prerrogativas alargadas) a fim de facilitar o **cumprimento das obrigações em matéria de interceção legal**.

37. Sujeitar os prestadores de serviços de comunicações eletrónicas (conforme definidos no Código Europeu das Comunicações Eletrónicas[57]) às mesmas regras aplicáveis aos prestadores de serviços tradicionais.

38. Prosseguir a **harmonização dos quadros jurídicos nacionais de acesso aos dados em trânsito**[58] através de várias etapas:

    i. Assegurar que as obrigações de interceção legal estabelecidas nas legislações nacionais são **aplicáveis a um leque mais vasto de fornecedores de serviços de comunicações**, incluindo as categorias pertinentes de fornecedores de serviços Internet (e procurar inspirar-se, a este respeito, no pacote relativo às provas eletrónicas).

    ii. Procurar uma harmonização a nível dos Estados-Membros da UE com base em **princípios comuns acordados** (nomeadamente os que fazem parte do documento LEON – *Law Enforcement Operational Needs*) através de instrumentos jurídicos não vinculativos (por exemplo, uma recomendação da Comissão).

---

56 A iniciativa SIRIUS criou, em 2020, a rede SPoC SIRIUS que tem uma plataforma específica na Plataforma de Peritos da Europol. É atualmente composta por 39 autoridades de aplicação da lei provenientes de 22 países da UE e de 2 países terceiros.

57 Artigo 2.º, n.º 1, ponto 4, da Diretiva (UE) 2018/1972.

58 O conceito de «dados em trânsito» pode abranger os casos em que a recolha de dados não é efetuada durante o trânsito, mas quando os dados de comunicação estão prestes a ser enviados ou foram recebidos (por vezes definidos como «dados em tempo real»).

iii. Refletir sobre uma **definição de interceção legal** no contexto alargado dos serviços de comunicações na Internet, distinguindo também entre interceção legal de dados não relacionados com o conteúdo e de dados de conteúdo.

iv. Com base numa análise mais aprofundada e numa avaliação de impacto, nomeadamente do ponto de vista dos direitos fundamentais e tendo em conta a soberania dos Estados em matéria penal, poderá eventualmente apresentar-se uma iniciativa da UE em matéria de interceção legal (que consista em instrumentos jurídicos não vinculativos ou instrumentos jurídicos vinculativos), inspirando-se no trabalho realizado no domínio das provas eletrónicas e envidando esforços com vista à celebração de acordos internacionais e bilaterais (por exemplo, com os Estados Unidos). Essa iniciativa teria de assegurar que os princípios do «acesso lícito desde a conceção» fossem devidamente aplicados pelas partes interessadas pertinentes (por exemplo, os serviços de comunicações eletrónicas) de modo a cumprir requisitos definidos, nomeadamente para permitir o acesso a dados não cifrados, quando tal seja considerado necessário e proporcionado.

39. Ajustar o **conceito de jurisdição territorial sobre os dados** para fazer face a potenciais conflitos de leis com outras jurisdições. Nos casos em que o nexo seja nacional (por exemplo, um crime cometido num Estado-Membro por um criminoso que se situa no mesmo Estado-Membro), deverá ser possível estabelecer uma medida de interceção, no quadro do direito processual nacional, que estabeleça requisitos e garantias, sem ter de recorrer a um instrumento de cooperação transfronteiriça.

40. Explorar a forma como a **decisão europeia de investigação (DEI)** poderia apoiar melhor a eficácia dos pedidos de interceção lícita transfronteiras, melhorando a segurança jurídica, reduzindo os atrasos na resposta aos mandados e promovendo uma utilização uniforme em toda a Europa da DEI e da Convenção de Budapeste do Conselho da Europa sobre o Cibercrime, a fim de colmatar as lacunas existentes em matéria de acesso aos dados.

41. Refletir sobre as **salvaguardas necessárias** quando a interceção legal se aplica a prestadores de serviços de comunicações não tradicionais. Alguns peritos sugerem que esta medida de investigação só deverá dizer respeito a comunicações que tenham lugar após a receção de um pedido legal das autoridades. Além disso, as medidas não deverão implicar a obrigação de os prestadores de serviços adaptarem os seus sistemas de TIC de uma forma que tenha um impacto negativo na cibersegurança dos seus utilizadores.

42. Adotar regras mínimas a nível da UE que permitam a admissibilidade mútua entre os Estados-Membros dos **elementos de prova** obtidos a partir de medidas de interceção legal contra prestadores não cooperantes e que prevejam a admissibilidade também em caso de recurso a medidas intrusivas, na medida do necessário para facilitar o reconhecimento mútuo de sentenças e decisões judiciais e a cooperação policial e judiciária em matéria penal.