

Pacote e-Evidence:

o que muda para os
prestadores de serviços digitais?

```
extends Node {  
  constructor() {  
    this._filter = new LPF.Filter({cutoff: 1000});  
    this._input = new InputSocket('audio_in');  
    this._output = new OutputSocket('audio_out');  
  }  
  process(audio) {  
    this._input.write(audio);  
    this._filter.process(this._input.read());  
    this._output.write(this._filter.read());  
  }  
}
```

Índice

1. Principais destaques	→ Saiba mais
1.1 O que é o Pacote e-Evidence?	→ Saiba mais
2. Enquadramento do regime	→ Saiba mais
2.1 O que integra o Pacote e-Evidence?	→ Saiba mais
2.2 O que muda face ao regime anterior?	→ Saiba mais
2.3 Porque é o regime particularmente relevante para empresas digitais?	→ Saiba mais
3. O novo regime: como funciona o novo mecanismo europeu de obtenção de prova eletrónica?	→ Saiba mais
3.1 Que categorias de dados podem ser pedidos?	→ Saiba mais
3.2 Que prestadores podem estar abrangidos?	→ Saiba mais
3.3 Quem deve receber e executar as ordens?	→ Saiba mais
3.4 Pode uma empresa recusar ou opor-se ao cumprimento?	→ Saiba mais
4. Implementação em Portugal	→ Saiba mais
4.1 Que autoridades assumem funções em Portugal?	→ Saiba mais
4.2 O que deve estar operacional até fevereiro de 2027?	→ Saiba mais
5. Consequências do incumprimento	→ Saiba mais
5.1 Medida da coima	→ Saiba mais
5.2 Como evitar o incumprimento	→ Saiba mais
6. O que fazer agora?	→ Saiba mais

Desde 18 de agosto de 2026, uma autoridade judiciária de qualquer Estado-Membro pode enviar diretamente a um prestador de serviços digitais uma ordem para produzir ou conservar dados, sem passar pelos canais clássicos de cooperação judiciária. Em Portugal, a Lei n.º 55/2026 completa o regime, com coimas que podem chegar a 2% do volume de negócios mundial. O prazo para designar o destinatário das ordens termina a 25 de fevereiro de 2027.

1. Principais destaques

- Já em aplicação: o Regulamento (UE) 2023/1543 aplica-se desde 18 de agosto de 2026.
- Prazos curtos: 10 dias para revelar dados e 8 horas em caso de emergência. A conservação dura 60 dias, prorrogáveis por mais 30.
- Âmbito extraterritorial: o critério de aplicação é a prestação de serviços na União, com uma “ligação substancial” a um Estado-Membro; não é o local da sede ou dos servidores.
- Destinatário obrigatório: é necessário designar um estabelecimento ou nomear um representante legal e comunicá-lo até 25 de fevereiro de 2027.
- Sanções elevadas: a responsabilidade é solidária, há coimas para infrações muito graves até 2% do volume de negócios mundial e pode ser aplicada uma sanção pecuniária compulsória de até EUR 3.000.000.

Qualquer Estado-Membro pode enviar a um prestador de serviços digitais uma ordem para produzir ou conservar dados, sem passar pelos canais clássicos de cooperação judiciária.

1.1. O QUE É O PACOTE E-EVIDENCE?

A crescente digitalização da economia fez da prova eletrónica um elemento central das investigações criminais. Contudo, os dados relevantes para uma investigação encontram-se frequentemente armazenados por prestadores de serviços localizados em diferentes Estados-Membros ou até fora da União Europeia, tornando a sua obtenção mais complexa e morosa.

Foi neste contexto que a União Europeia aprovou o **Pacote e-Evidence**, introduzindo um novo mecanismo para a obtenção e conservação transfronteiriça de prova eletrónica em processos penais. O objetivo é permitir uma cooperação mais rápida e eficaz entre autoridades judiciárias e prestadores de serviços, através de ordens diretamente dirigidas ao estabelecimento designado ou ao representante legal do prestador.

Embora tenha sido concebido para fins de investigação criminal, o novo regime tem um impacto direto nas empresas que armazenam, tratam ou disponibilizam dados em formato eletrónico. Em particular, poderá ser relevante para prestadores de serviços de comunicações eletrónicas, *cloud computing*, SaaS, plataformas digitais, *marketplaces*, redes sociais e serviços de alojamento.

A aplicabilidade do regime não depende necessariamente da localização da sede ou dos servidores da empresa, mas da forma como os serviços são disponibilizados na União Europeia e da existência de uma ligação substancial a um ou mais Estados-Membros. Por essa razão, muitas organizações poderão estar abrangidas sem o anteciparem.

2. Enquadramento do regime

2.1. O QUE INTEGRA O PACOTE E-EVIDENCE?

O Pacote e-Evidence assenta em três instrumentos europeus complementares:

- O **Regulamento (UE) 2023/1543**, aplicável desde 18 de agosto de 2026, que criou as Ordens Europeias de Produção e de Conservação de prova eletrónica;
- A **Diretiva (UE) 2023/1544**, que harmonizou a obrigação de designar um estabelecimento designado ou representante legal para receber e executar essas ordens, com prazo de transposição até 18 de fevereiro de 2026; e
- O **Regulamento de Execução (UE) 2025/1550**, que estabelece as regras técnicas para as comunicações eletrónicas através da infraestrutura e-CODEX.

Em Portugal, a Diretiva (UE) 2023/1544 foi transposta pela **Lei n.º 55/2026, de 20 de agosto**, que entrou em vigor em 25 de agosto de 2026. A Lei n.º 55/2026 cria também o regime sancionatório da Diretiva e do Regulamento e altera a Lei n.º 144/99 (cooperação judiciária internacional em matéria penal) e a Lei n.º 109/2009 (Lei do Cibercrime).

2.2. O QUE MUDA FACE AO REGIME ANTERIOR?

Até agora, o acesso a dados detidos por prestadores de serviços localizados noutro Estado-Membro ou fora da União Europeia dependia, em regra, dos mecanismos tradicionais de cooperação judiciária internacional, que envolviam a intervenção de várias autoridades e podiam prolongar-se durante semanas ou meses.

O novo regime responde à crescente necessidade de obtenção célere de prova digital: permite que, em determinadas circunstâncias, uma autoridade judiciária de um Estado-Membro dirija diretamente uma ordem ao prestador ou representante situado noutro Estado-Membro.

Apesar da sua relevância, o Pacote e-Evidence vem complementar e não substituir os instrumentos tradicionais de cooperação judiciária internacional.

2.3. PORQUE É O REGIME PARTICULARMENTE RELEVANTE PARA EMPRESAS DIGITAIS?

Porque transforma a capacidade de responder a pedidos das autoridades numa obrigação regulada, sujeita a exigências organizacionais, operacionais e legais específicas.

As empresas potencialmente abrangidas passam a ter de assegurar a existência de um destinatário formal para receção das ordens, mecanismos internos de validação e resposta, procedimentos de preservação de dados e capacidade para cumprir prazos particularmente exigentes, que em determinadas situações podem ser medidos em horas.

3. O novo regime: como funciona o novo mecanismo europeu de obtenção de prova eletrónica?

O Regulamento (UE) 2023/1543 veio permitir que determinadas autoridades judiciais de um Estado-Membro solicitem diretamente a prestadores de serviços abrangidos a *produção ou preservação de dados relevantes para uma investigação criminal, reduzindo significativamente a dependência dos mecanismos tradicionais de cooperação judiciária internacional*.

O novo regime assenta, nomeadamente, em dois instrumentos principais:

- o a **Ordem Europeia de Produção (“OEP”)** permite exigir a **transmissão de dados já armazenados pelo prestador de serviços**, em regra no prazo de 10 dias ou, em emergência, no prazo máximo de 8 horas;
- o a **Ordem Europeia de Conservação (“OEC”)**, com natureza cautelar, permite exigir a **preservação dos dados identificados** – por 60 dias, prorrogáveis por mais 30 dias, ou até à produção se for confirmado um pedido subsequente –, evitando a sua alteração ou eliminação até que sejam posteriormente solicitados pelas autoridades competentes.

3.1. QUE CATEGORIAS DE DADOS PODEM SER PEDIDOS?

Importa distinguir quatro categorias de dados sobre os quais podem incidir os pedidos, organizadas por grau crescente de intrusividade, com requisitos diferenciados de emissão:

- o Dados de assinante;
- o Dados para identificação do utilizador;
- o Dados de tráfego;
- o Dados de conteúdo.

A categoria de dados em causa influencia as condições de emissão da ordem, o nível de controlo judicial exigido e as garantias aplicáveis.

3.2. QUE PRESTADORES PODEM ESTAR ABRANGIDOS?

O âmbito de aplicação do regime é deliberadamente amplo. Não se limita às grandes plataformas tecnológicas globais, nem aos operadores tradicionais de comunicações eletrónicas.

O Regulamento aplica-se a prestadores que ofereçam serviços na União Europeia, incluindo prestadores de serviços de comunicações eletrónicas, serviços de nomes de domínio de Internet e numeração IP, ou outros serviços que permitam comunicação entre utilizadores ou conservação ou tratamento de dados em nome dos utilizadores, quando essa conservação seja componente determinante do serviço.

O Regulamento aplica-se a prestadores de serviços de comunicações eletrónicas, serviços de nomes de domínio de Internet e numeração IP ou outros serviços que permitam comunicação entre utilizadores ou conservação ou tratamento de dados em nome dos utilizadores.

O regime pode aplicar-se a prestadores estabelecidos fora da União Europeia quando ofereçam serviços na União e possuam uma ligação substancial a pelo menos um Estado-Membro.

Ficam excluídos os serviços financeiros e os serviços em que o armazenamento não é componente essencial do serviço prestado. Além disso, a Diretiva não se aplica a prestadores estabelecidos no território de um único Estado-Membro que ofereçam serviços exclusivamente nesse território e a Dinamarca não participa no regime.

A análise deve, assim, ser feita caso a caso, porque uma mesma organização pode prestar simultaneamente serviços abrangidos e serviços não abrangidos pelo regime.

3.3. QUEM DEVE RECEBER E EXECUTAR AS ORDENS?

Um dos pilares do novo regime consiste na identificação de um destinatário formal responsável por receber, gerir e assegurar o cumprimento das ordens emitidas pelas autoridades competentes.

Para esse efeito, os prestadores que ofereçam serviços abrangidos devem nomear um *estabelecimento designado ou um representante legal. Em ambos os casos, o destinatário deverá estar estabelecido num Estado-Membro onde os serviços sejam oferecidos e onde possa ser objeto de procedimentos de execução. O estabelecimento designado ou representante legal deve dispor de poderes, recursos e acesso efetivo à informação necessários para receber e analisar ordens, identificar e preservar os dados solicitados, comunicar com as autoridades competentes e, quando aplicável, invocar fundamentos de impossibilidade ou de não execução.*

Em Portugal, a designação deve ser feita até 25 de fevereiro de 2027. A Diretiva previa a designação até 18 de agosto de 2026. O prazo português mais longo deve-se à transposição tardia. Se o destinatário for designado noutro Estado-Membro, aplicam-se a lei e os prazos desse Estado-Membro.

Por sua vez, o Regulamento (UE) 2023/1543 é diretamente aplicável desde 18 de agosto de 2026. Isto significa que as entidades abrangidas já estão sujeitas às ordens regularmente transmitidas.

Em Portugal, a designação deve ser feita até 25 de fevereiro de 2027

3.4. PODE UMA EMPRESA RECUSAR OU OPOR-SE AO CUMPRIMENTO?

Por regra, os destinatários não podem recusar unilateralmente o cumprimento. A receção de uma Ordem Europeia de Produção ou de Conservação exige sempre uma atuação por parte do prestador de serviços, dentro dos prazos aplicáveis. A ordem não deve ser ignorada, mesmo quando existam dúvidas quanto à sua validade ou exequibilidade. Note-se ainda que, no caso de dados de tráfego e de conteúdo, o Regulamento prevê a notificação da autoridade do Estado de execução, que pode invocar fundamentos de recusa.

No entanto, o Regulamento prevê situações em que o destinatário pode solicitar esclarecimentos adicionais ou comunicar fundamentadamente à autoridade emissora a impossibilidade de execução da ordem, bem como mecanismos específicos para os casos em que o seu cumprimento entre em conflito com obrigações impostas pela legislação de países terceiros.

Esta matéria assume particular relevância para grupos multinacionais sujeitos simultaneamente ao regime e-Evidence e a outros enquadramentos legais, como o *Stored Communications Act* e o *CLOUD Act* norte-americanos ou restrições à divulgação de informação previstas por ordenamentos jurídicos de países terceiros. O acordo UE-EUA sobre acesso a prova eletrónica continua em negociação e ainda não foi concluído. Por essa razão, sempre que existam dúvidas quanto à validade da ordem, à sua exequibilidade ou à compatibilidade com outras obrigações legais aplicáveis, é aconselhável proceder a uma análise jurídica especializada antes de adotar qualquer posição perante a autoridade emissora.

4. Implementação em Portugal

4.1. QUE AUTORIDADES ASSUMEM FUNÇÕES EM PORTUGAL?

- **ANACOM:** autoridade central para as comunicações relativas aos estabelecimentos designados e representantes legais. Também fiscaliza, instaura os processos e aplica coimas e sanções acessórias;
- **Procuradoria-Geral da República:** autoridade central para efeitos do Regulamento;
- **Autoridades judiciais:** emitem, validam e executam as ordens.

4.2. O QUE DEVE ESTAR OPERACIONAL ATÉ FEVEREIRO DE 2027?

O prazo de **25 de fevereiro de 2027** respeita apenas ao cumprimento, pelos prestadores que já ofereciam serviços na União Europeia em 18 de fevereiro de 2026, da obrigação de designar um estabelecimento ou nomear um representante legal e de o comunicar à autoridade central competente. As restantes obrigações aplicam-se desde 18 de agosto de 2026.

Em termos práticos, as organizações abrangidas devem assegurar desde já, pelo menos, os seguintes elementos:

- **Destinatário formal identificado**, sem prejuízo do prazo legal aplicável à sua designação ou nomeação, dotado dos poderes e recursos necessários para receber e executar ordens;
- **Procedimento interno de receção, validação e tratamento de ordens**, com responsabilidades e fluxos de decisão claramente definidos;
- **Equipa jurídica ou mecanismo de verificação especializado**, capaz de analisar rapidamente questões de validade, âmbito ou conflitos normativos;

- **Inventário atualizado dos sistemas, aplicações e categorias de dados**, que permita identificar e localizar a informação relevante sem demora;
- **Mecanismos de preservação urgente de dados**, aptos a responder a Ordens Europeias de Conservação nos prazos exigidos;
- **Testes periódicos e exercícios internos de resposta**, que permitam validar a eficácia dos procedimentos implementados;
- **Capacidade técnica para utilizar os canais de comunicação aplicáveis**, incluindo, em especial, os meios alternativos admitidos pelo Regulamento e, quando se tornar obrigatória, a integração com a infraestrutura e-CODEX.



5. Consequências do incumprimento

5.1. MEDIDA DA COIMA

Para as pessoas coletivas, as coimas podem atingir 2% do volume de negócios total mundial do exercício anterior, nas falhas de conservação ou transmissão de dados, e 1%, na falta de medidas de confidencialidade e segurança.

Por outro lado, o incumprimento das obrigações decorrentes do Pacote pode, ainda, determinar a aplicação de uma sanção pecuniária compulsória diária de até EUR 3.000.000, por período não superior a 30 dias.

Além disso, pela prática de contraordenações muito graves pode ainda ser aplicada a sanção acessória de interdição do exercício da atividade de prestador de serviços em território nacional por período máximo de dois anos. O desrespeito desta interdição pode constituir crime de desobediência qualificada.

O prestador e o estabelecimento designado ou representante legal são solidariamente responsáveis pelo cumprimento das obrigações de execução. Consequentemente, a simples existência formal de um representante legal ou de um estabelecimento designado não elimina a necessidade de assegurar uma coordenação efetiva entre as diferentes entidades envolvidas

5.2. COMO EVITAR O INCUMPRIMENTO

As organizações potencialmente abrangidas deverão avaliar se os seus serviços se encontram dentro do âmbito de aplicação do regime, identificar o modelo adequado de estabelecimento designado ou representante legal, rever os seus procedimentos internos e testar a sua capacidade de resposta a ordens de produção e conservação de prova eletrónica. Em muitos casos, esta análise exigirá uma avaliação jurídica e operacional multidisciplinar que permita compreender a exposição concreta da organização e definir um plano de implementação proporcional ao respetivo perfil de risco.

A sanção acessória de interdição do exercício da atividade de prestador de serviços em território nacional por período máximo de dois anos.

6. O que fazer agora?

Independentemente do número de ordens que cada organização venha a receber, uma conclusão parece impor-se: com o Pacote eEvidence, a capacidade de responder às autoridades judiciais deixa de ser uma questão de boa vontade e passa a ser uma obrigação legal, com prazos que se contam em dias ou em horas e com sanções relevantes em caso de incumprimento.

Para os prestadores de serviços digitais que operam na União, é essencial avaliar, serviço a serviço, se a atividade está abrangida pelo regime e, sendo o caso, designar e dotar de meios o estabelecimento designado ou o representante legal até 25 de fevereiro de 2027. É igualmente essencial adotar os procedimentos internos que permitam receber, validar, conservar e transmitir dados nos prazos legais, bem como identificar atempadamente eventuais conflitos com o direito de países terceiros ou com as regras de proteção de dados.

Em matéria de prova eletrónica, quem se prepara antes de receber a primeira ordem define também, muitas vezes, a qualidade e a segurança da sua resposta. Num contexto de crescente exigência regulatória, um modelo de resposta testado na prática é hoje um mitigador crítico de risco sancionatório, operacional e reputacional. A PLMJ está disponível para apoiar cada organização na avaliação da sua exposição concreta e na definição de um plano de implementação ajustado ao seu perfil de risco.

Sobre a PLMJ

→ Quem somos

“PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us.”

CLIENT REFERENCE FROM
CHAMBERS AND PARTNERS

Sobre Resolução de Litígios

→ O que fazemos

KEY CONTACTS



Paulo Farinha
Alves

Sócio

+351 213 197 530
paulo.farinhaalves@plmj.pt



Raquel Cardoso
Nunes

Associada Coordenadora

(+351) 213 197 566
raquel.cardosonunes@plmj.pt

