POLÍCIA JUDICIÁRIA

CENTRO DE ESTUDOS JUDICIÁRIOS

Pesquisa e apreensão de dados em ambiente digital

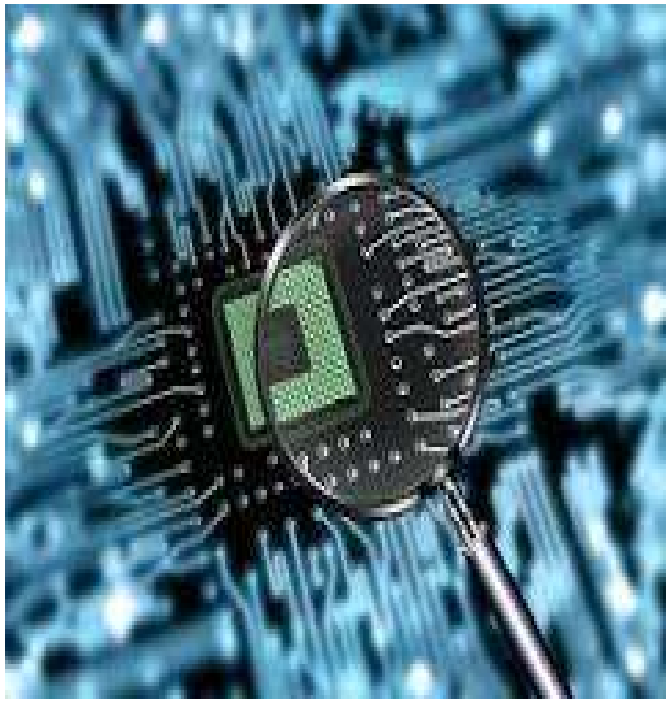
Agenda

1. **Noção e recolha de Prova Digital**
2. **Legislação relevante**
3. **Exemplos práticos**


POLICE
DIGITAL FORENSICS

Prova Digital

Refere-se a informação gerada, armazenada ou transmitida eletronicamente que possa ser recolhida, preservada, analisada e apresentada em processos judiciais para suportar uma investigação criminal.



Características da Prova Digital

- **Imaterialidade** (dados intangíveis ≠ de objetos físicos)
- **Volatilidade** (facilmente apagada ou modificada, intencionalmente ou por fatores externos como atualizações de sistemas, perda de energia, temperatura, humidade, eletromagnetismo)
- **Complexidade técnica** (requer competências técnicas para ser identificada, recolhida e interpretada)
- **Integridade/Autenticidade** (não deve sofrer alterações aquando da recolha e tratamento – utilização de funções *hash*)

Princípios da Prova Digital

- **Admissível** (conforme à lei vigente)
- **Autêntica** (na relação entre o indício e o evento)
- **Completa** (deve ser imparcial e não tendenciosa)
- **Confiável** (recolha e tratamento não deve colocar em causa a sua veracidade)
- **Acreditável** (compreensível e plausível)

Recolha da Prova Digital

Deve ser feita com o menor impacto possível no sistema-alvo (particularmente difícil em sistemas "vivos")

Impacto deve ser avaliado (não pode ser evitado?) e documentado (devem sempre ficar reduzidos a escrito todos os passos tomados)

Prova deve ser recolhida no sentido do mais volátil para o menos (memória RAM, interfaces de rede, processos em execução no sistema, áreas *swap* e *hiberfile*, …, discos rígidos, dados na *cloud* e *backup* externo)

Pesquisa e apreensão de dados

O CPP consagra o regime de buscas e apreensões, como meios de obtenção de prova (Art.º 174º a 186º), aplicados a **espaços físicos**. As apreensões visam coisas ou objetos **tangíveis**.

Nem umas nem outras se adaptam às realidades tecnológicas.

Não são suscetíveis de aplicação na realização de buscas em sistemas informáticas ou na apreensão de dados informáticos.

Os sistemas informáticos **não são espaços físicos** e os dados **não são objetos tangíveis**.

Pesquisa e apreensão de dados

Lei do Cibercrime veio consagrar buscas e pesquisas em sistemas informáticos e apreensões de dados informáticos, como meios de aquisição ou obtenção de prova, nos respetivos Art.º 15º a 17º.

Mecanismos que podem ser usados na investigação da generalidade dos tipos de crimes de acordo com o Art.º 11º, n.º 1, podendo recorrer-se a estas medidas de investigação quando estiverem em causa crimes, previsto na LCC, cometidos por meio de um sistema informático ou crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

Lei n.º 109/2009

Art.º 15.º

Pesquisa de dados informáticos

Quando se tornar necessário obter dados informáticos armazenados num determinado sistema informático, a autoridade judiciária competente (em regra o MP), autoriza ou ordena por despacho (**até 30 dias**) que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

Lei n.º 109/2009

Art.º 15.º, n.º 3

O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) Existir consentimento de quem tiver a disponibilidade ou controlo desses dados, o qual deverá ficar documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada - ver definições do Art.º 1.º, als. i), j) e m) do CPP - quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

Lei n.º 109/2009

Art.º 15.º, n.º 4

Quando o OPC proceder à pesquisa informática (entenda-se sem despacho da autoridade judiciária):

- No caso previsto na alínea b), a realização da diligência é, **sob pena de nulidade**, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;
- Em ambos os casos é elaborado e remetido à autoridade judiciária competente um relatório, onde deve ser mencionado, de forma resumida, as circunstâncias que levaram à realização da pesquisa, outras circunstâncias consideradas relevantes e o respetivo resultado, conforme previsto no Art.º 253.º do CPP.

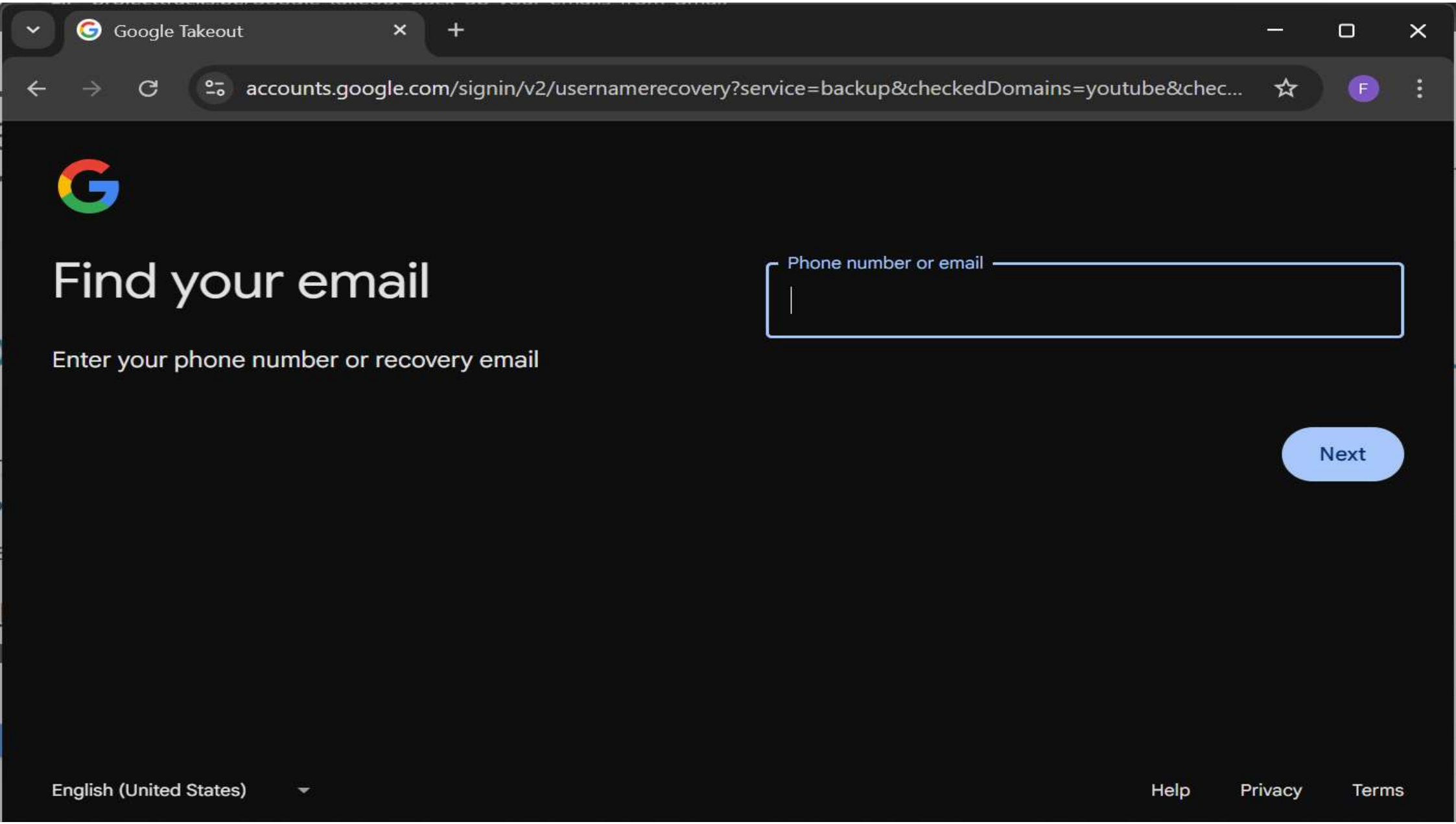
Lei n.º 109/2009

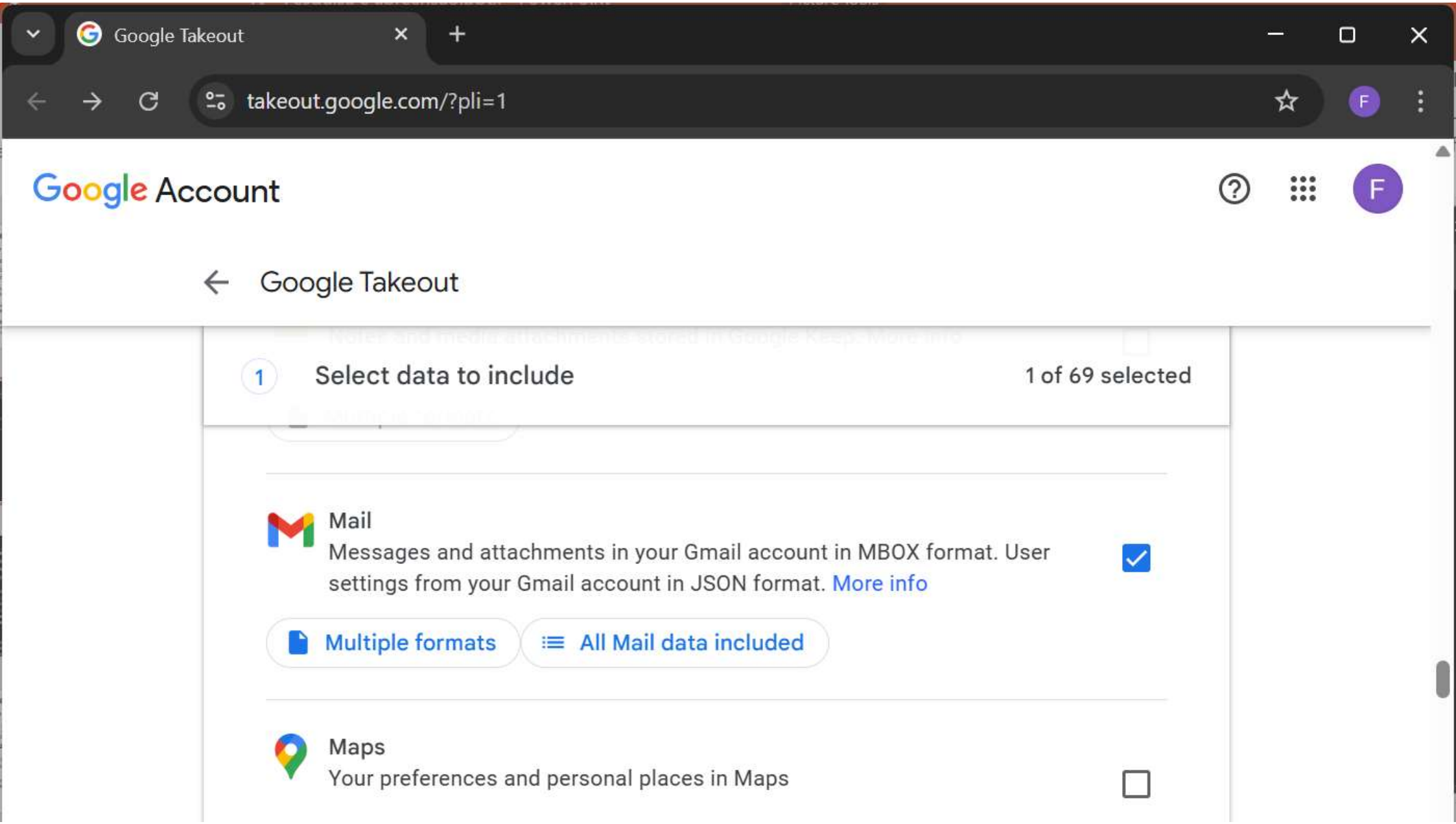
Art.º 15.º, n.º 5

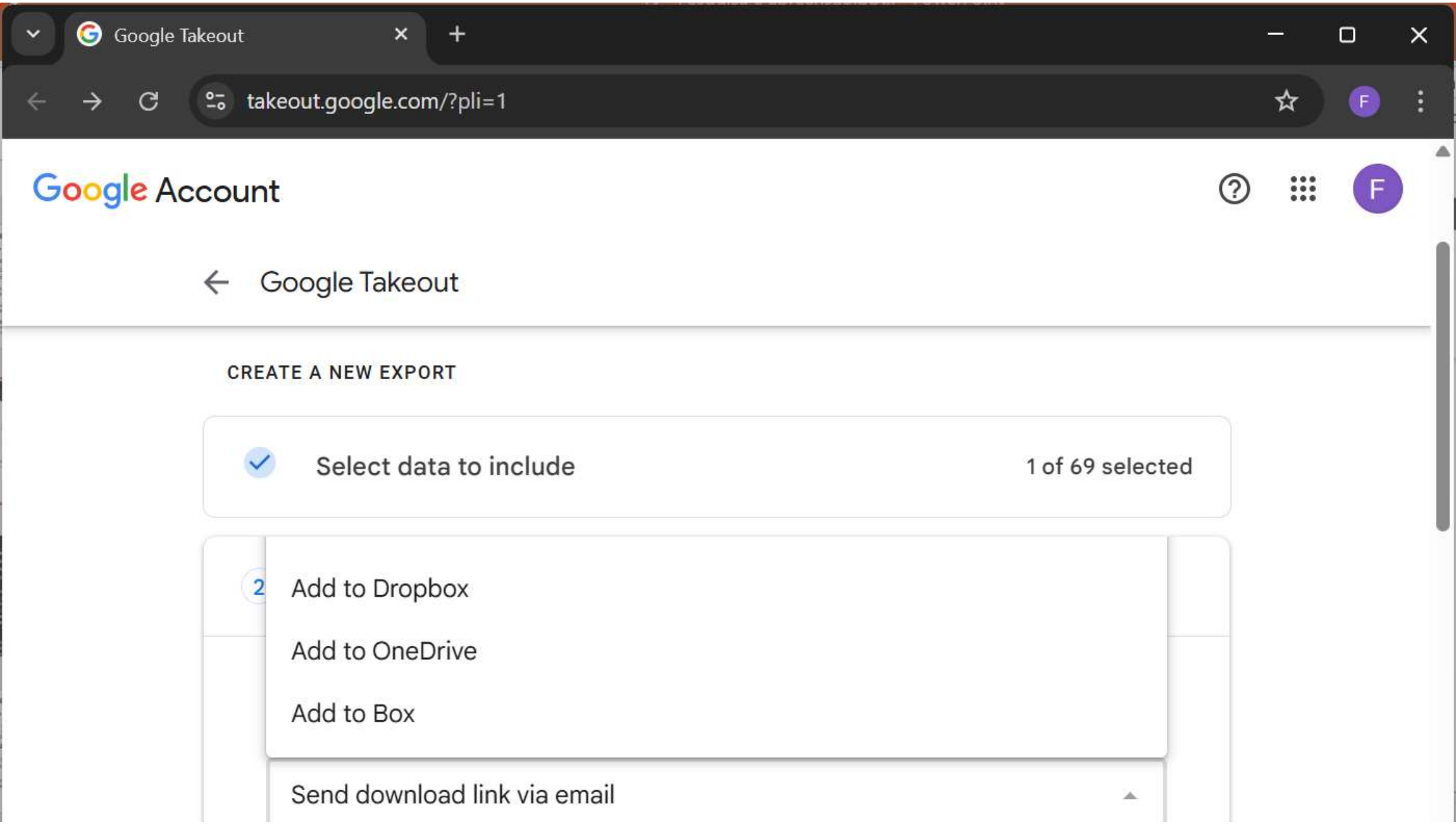
Caso surjam razões para crer que os dados procurados se encontram noutro computador ou sistema informático, mas são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser relizada.

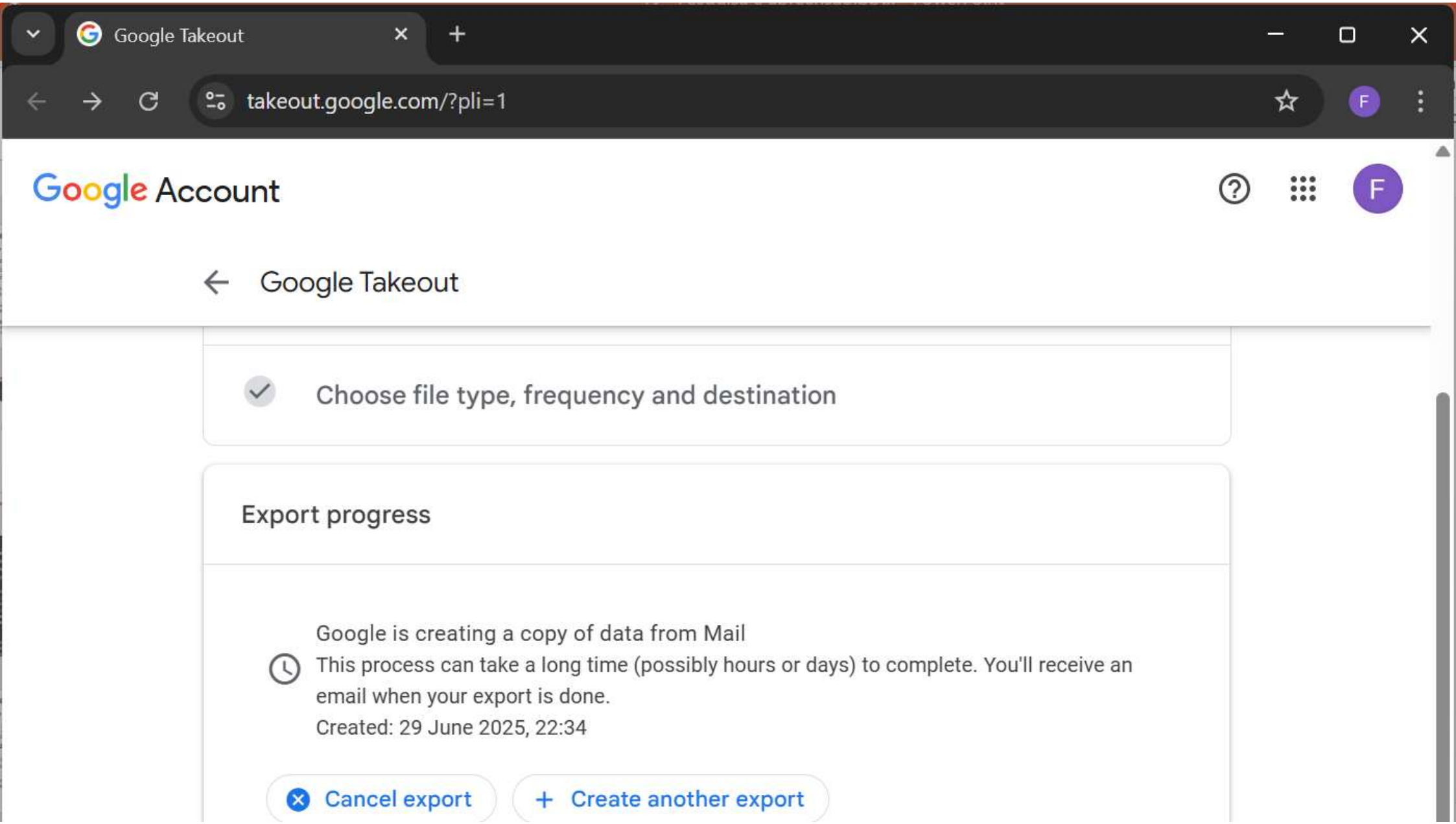
Introduz o conceito de buscas, neste caso pesquisas à distância. **Exemplos**:

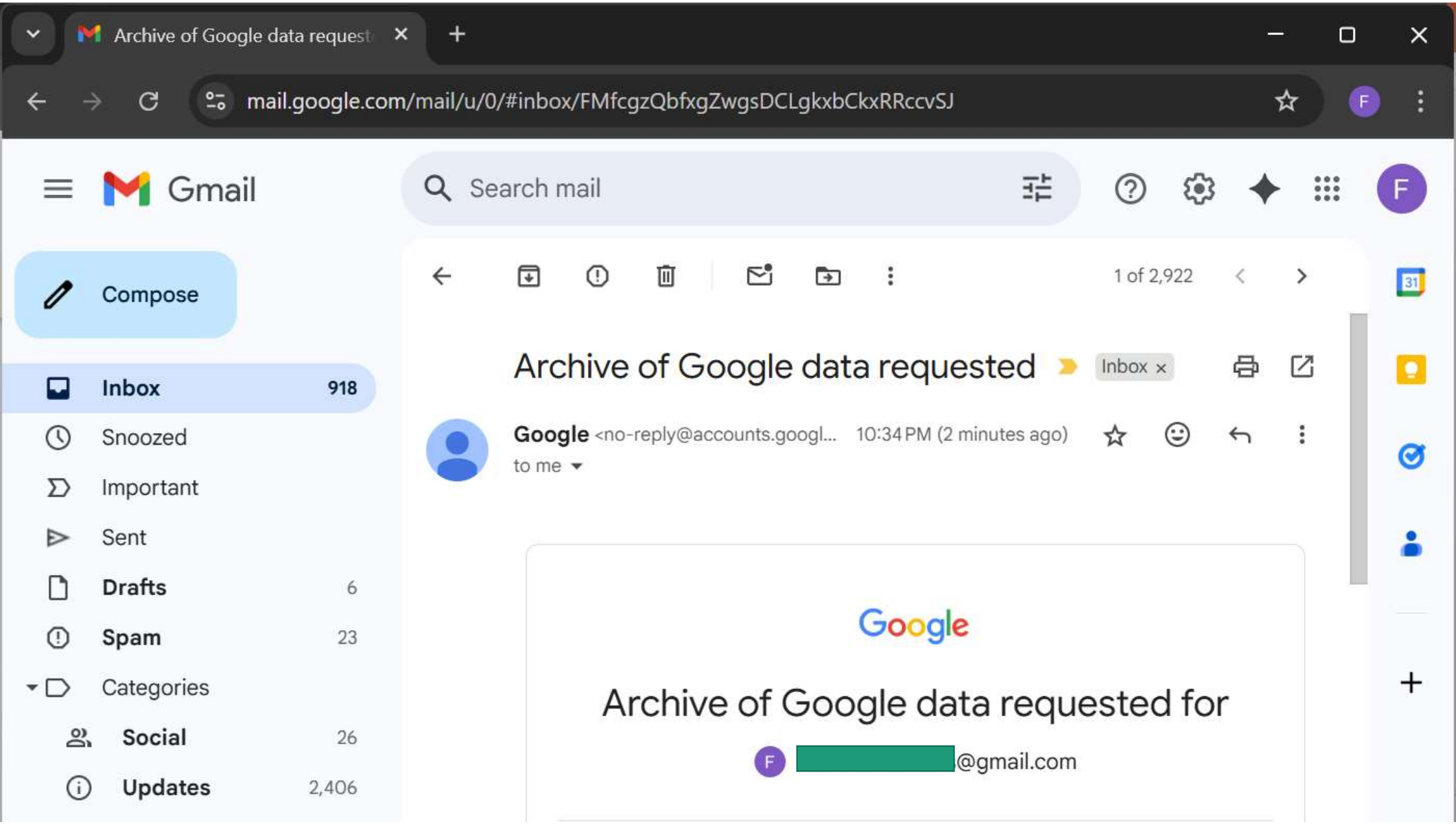
- permite o acesso a servidores de uma empresa, a partir de terminais existentes na empresa, que se encontrem física e/ou geograficamente distantes.
- permite o acesso a contas de *webmail* ou de redes sociais, desde que o dispositivo de onde se acede tenha legitimamente acesso às mesmas.
- permite o acesso a sistemas informáticos controlados pelos suspeitos, a partir de um dos dispositivos na posse destes, que se encontrem física e/ou geograficamente distantes.

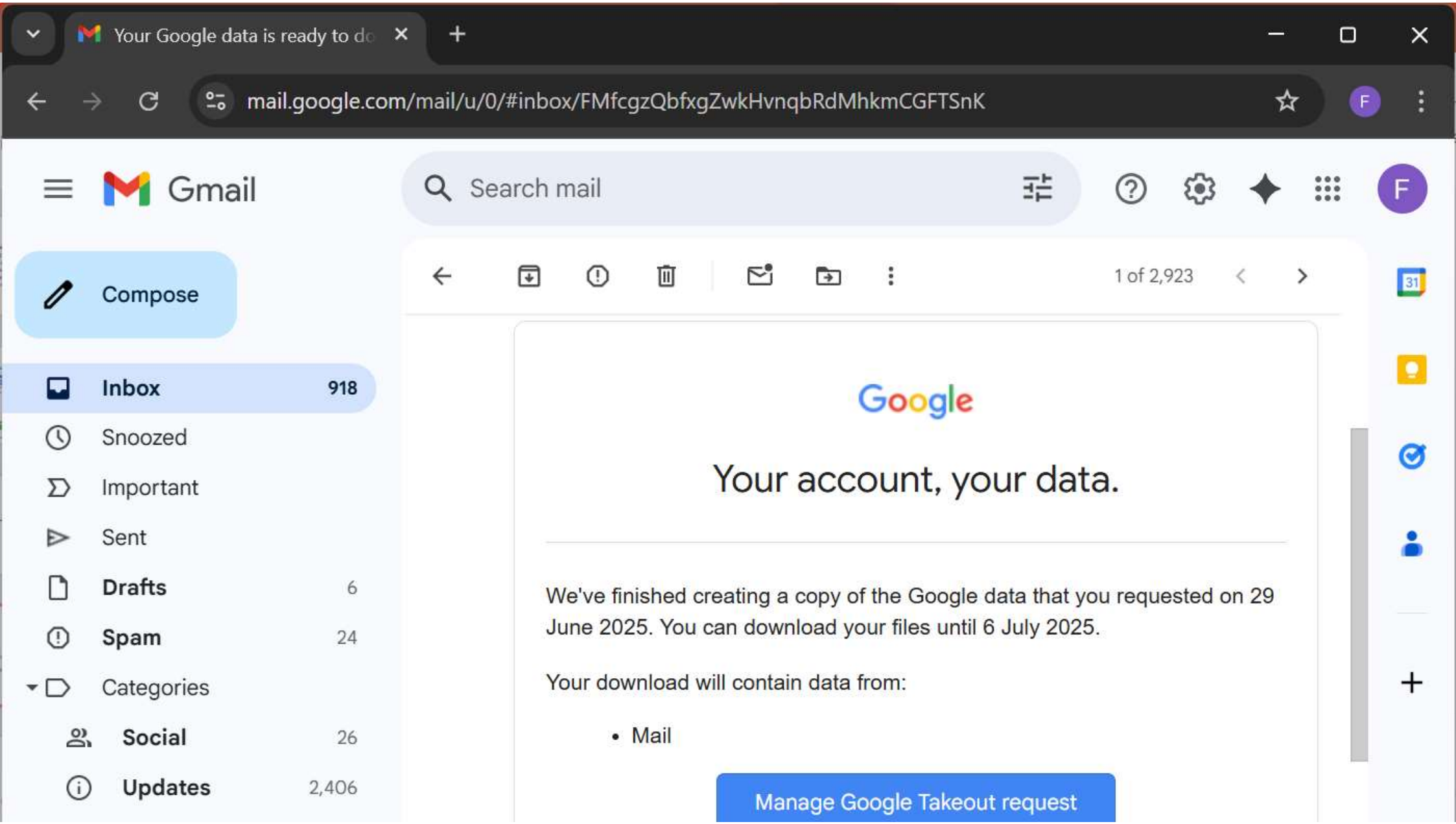

Google Takeout
accounts.google.com/signin/v2/usernamerecovery?service=backup&checkedDomains=youtube&chec...
Find your email
Enter your phone number or recovery email
Phone number or email
Next
English (United States)
Help
Privacy
Terms

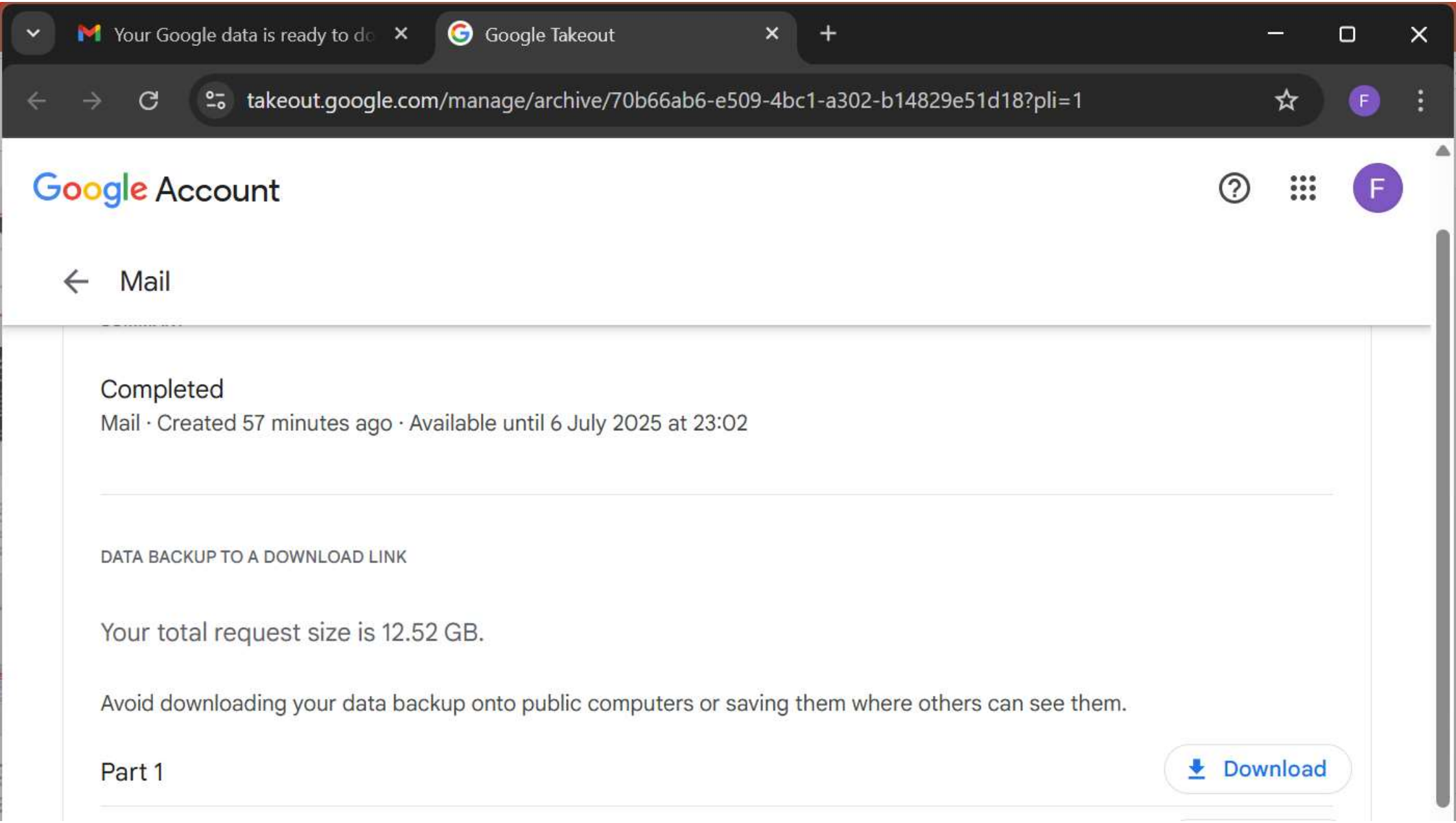

Google Takeout
takeout.google.com/?pli=1
Google Account
F
Google Takeout
1
Select data to include
1 of 69 selected
Mail
Messages and attachments in your Gmail account in MBOX format. User settings from your Gmail account in JSON format. More info
Multiple formats
All Mail data included
Maps
Your preferences and personal places in Maps


Google Takeout
takeout.google.com/?pli=1
Google Account
F
Google Takeout
CREATE A NEW EXPORT
Select data to include
1 of 69 selected
2
Add to Dropbox
Add to OneDrive
Add to Box
Send download link via email


Google Takeout
takeout.google.com/?pli=1
Google Account
F
Google Takeout
Choose file type, frequency and destination
Export progress
Google is creating a copy of data from Mail
This process can take a long time (possibly hours or days) to complete. You'll receive an email when your export is done.
Created: 29 June 2025, 22:34
Cancel export
Create another export


Archive of Google data request
mail.google.com/mail/u/0/#inbox/FMfcgzQbfxgZwgsDCLgkxbCkxRRccvSJ
Gmail
Search mail
Compose
Inbox 918
Snoozed
Important
Sent
Drafts 6
Spam 23
Categories
Social 26
Updates 2,406
1 of 2,922
Archive of Google data requested
Inbox ×
Google <no-reply@accounts.googl... 10:34 PM (2 minutes ago)
to me
Google
Archive of Google data requested for
@gmail.com


Your Google data is ready to do
mail.google.com/mail/u/0/#inbox/FMfcgzQbfxgZwkHvnqbRdMhkmCGFTSnK
Gmail
Search mail
Compose
Inbox 918
Snoozed
Important
Sent
Drafts 6
Spam 24
Categories
Social 26
Updates 2,406
1 of 2,923
Google
Your account, your data.
We've finished creating a copy of the Google data that you requested on 29 June 2025. You can download your files until 6 July 2025.
Your download will contain data from:
Mail
Manage Google Takeout request


Your Google data is ready to do
Google Takeout
takeout.google.com/manage/archive/70b66ab6-e509-4bc1-a302-b14829e51d18?pli=1
Google Account
F
Mail
Completed
Mail · Created 57 minutes ago · Available until 6 July 2025 at 23:02
DATA BACKUP TO A DOWNLOAD LINK
Your total request size is 12.52 GB.
Avoid downloading your data backup onto public computers or saving them where others can see them.
Part 1
Download

Expresso

JUSTIÇA

Durante anos, Sergey Gusev lesou milhares de pessoas a partir do seu portátil – até o FBI e a PJ baterem à porta da sua casa em Gaia

O Tribunal da Relação do Porto revogou, esta quarta-feira, a absolvição de um pirata informático luso-russo, que havia sido denunciado pela polícia norte-americana (FBI) à Polícia Judiciária. Sergey Gusev estava acusado de gerir um site que vendia dados de contas bancárias e credenciais de cartões de crédito.

César Castro
Jornalista

Relacionados

→ **Pirata russo de Gaia denunciado pelo FBI foi absolvido. Estava preso há um ano**

→ **Esconderijo em Gaia era centro nevrálgico de hacker luso-russo**

O homem, residente em Vila Nova de Gaia, havia sido absolvido em julho do ano passado, tal como o JN noticiou, mas o Ministério Público recorreu. E, por acórdão de hoje, o Tribunal da Relação do Porto revogou a decisão de primeira instância, condenando o arguido por um crime de **associação criminosa** e um crime de **branqueamento de capitais**, na pena única de **cinco anos e seis meses** de prisão efetiva.

O arguido terá ainda de pagar mais de 687 mil euros, que terá obtido como vantagem da atividade criminosa, ao Estado. Igualmente perdidos a favor deste vão ficar os 2.500 euros que tinham sido

Lei n.º 109/2009

Art.º 15.º, n.º 5

O quadro jurídico português permite às autoridades de justiça criminal aceder a dados armazenados num sistema remoto, mesmo que tal sistema esteja fisicamente no estrangeiro.

A aplicação do **Princípio da Disponibilidade** legitima o acesso a estes dados (provas).

Art.º 25º confere idêntica permissão a autoridades congéneres estrangeiras, quanto a dados fisicamente alojados em Portugal.

Os dados informáticos que venham a ser apreendidos por esta via constituem prova válida, por aplicação da regra geral do Art.º 125º do CPP.

Acórdão do Tribunal da Relação do Porto

5722/22.2T9AVR-A.P1
JTRP000
FRANCISCO MOTA RIBEIRO
CONVENÇÃO DE BUDAPESTE
LEI DO CIBERCRIME
INTERPRETAÇÃO DA LEI
ELEMENTOS ESSENCIAIS
JURISPRUDÊNCIA INTERNACIONAL
PRINCÍPIO DA TERRITORIALIDADE
SISTEMA INFORMÁTICO
DADOS PESSOAIS
ACESSO A DADOS
LEGALIDADE
RP202412115722/22.2T9AVR-A.P1
11/12/2024
UNANIMIDADE
S
1
RECURSO PENAL (CONFERÊNCIA)
NEGADO PROVIMENTO AO RECURSO INTERPOSTO PELAS ARGUIDAS
4. ª SECÇÃO CRIMINAL
.

I - Contextualizando-se a interpretação com um sentido atualista dos art.ºs 19º, 22º e 32º da Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001, à luz dos respetivos objeto e fim, tendo-se devidamente em conta os elementos sistemático e teleológico, assim como a jurisprudência internacional relevante, nomeadamente os Acórdão do Supremo Tribunal Federal Suíço, de 24/05/2017, e do Supremo Tribunal da Noruega, de 29/03/2019 (caso *Tidal*), cujos países são Partes naquela Convenção, não haverá violação do princípio da territorialidade no acesso e recebimento de dados informáticos armazenados em *Cloud Computing*, num servidor localizado em território estrangeiro, quando, de harmonia com a legislação interna, os dados pesquisados, ainda que localizados fora do respetivo território, o foram através de credenciais que em si permitiam o acesso legítimo a esses mesmos dados por parte da entidade investigada, a partir do seu próprio território, não assumindo ademais a busca informática realizada uma dimensão que pudesse materialmente pôr em causa o princípio da soberania de outro Estado.
II - O princípio da territorialidade, nos termos previstos na Convenção de Budapeste, assim como o princípio do primado do direito internacional convencional sobre o direito ordinário interno, não terão possibilidade de aplicação quando a busca informática a realizar tiver por objeto dados de um sistema informático situado num "espaço virtual" relativamente ao qual se desconhece o local geográfico das máquinas ou dos materiais físicos de suporte onde tal sistema informático e respetivos dados se encontram guardados, ou, conhecendo-se esse local, o respetivo país não tenha ratificado, aceitado ou aprovado aquela Convenção, nos termos dos art.ºs 2º da Convenção de Viena sobre o Direito dos Tratados e 36º da Convenção sobre o Cibercrime.
III – Concomitantemente não haverá qualquer questão de ilegalidade por confrontação de normas de direito internacional convencional com as normas de direito ordinário interno, e assim também qualquer violação do art.º 8º, nº 2, da Constituição da República Portuguesa.
IV - A determinação pelo Ministério Público, na qualidade de autoridade judiciária, no sentido de se proceder cautelarmente à realização de cópias digitalmente encriptadas, devidamente seladas, sendo uma delas para entregar ao Juiz de instrução criminal, de cujo conteúdo virá este a ter conhecimento em primeiro lugar, tendo em vista a

Lei n.º 109/2009

Art.º 15.º

Também as Autoridades de Polícia Criminal (APCs) da PJ têm competência para determinar a pesquisa em sistema informático, sempre que não seja possível, dada a situação de urgência e perigo na demora, aguardar pela decisão de autoridade judiciária.

A determinação da pesquisa informática, por APC, obedece à tramitação do CPP e tem de ser de imediato comunicada à autoridade judiciária titular do processo, para os efeitos e sob as cominações da lei processual penal.

Lei n.º 109/2009

Art.º 15.º

À pesquisa são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no CPP e no Estatuto do Jornalista (Art.º 15.º, n.º 6).

Deve constar do Auto de Busca e Apreensão a identificação dos equipamentos pesquisados, bem como o resultado da pesquisa, ainda que negativa.

Lei n.º 109/2009

Art.º 16.º

Apreensão de dados informáticos

Se no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

Lei n.º 109/2009

Art.º 16.º

O OPC pode efetuar apreensões, **sem prévia autorização da autoridade judiciária**, no decurso de pesquisa informática legitimamente ordenada e executada, bem como quando haja urgência ou perigo na demora.

Que deve ser descrita no Auto de Busca e Apreensão, conforme atrás referido.

Lei n.º 109/2009

Art.º 16.º

Caso sejam apreendidos dados ou documentos informáticos suscetíveis de **revelar dados pessoais ou íntimos**, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, **sob pena de nulidade** esses dados ou documentos **são apresentados ao juiz**, que ponderará a sua junção aos autos, tendo em conta os interesses do caso concreto.

Lei n.º 109/2009

Art.º 16.º

As apreensões efetuadas por OPC são sempre sujeitas a validação pela AJ, **no prazo máximo de 72 horas**.

As apreensões relativas a sistemas informáticos utilizados para o **exercício da advocacia** e das **atividades médica** e **bancária** estão sujeitas às regras e formalidades previstas no CPP.

Lei n.º 109/2009

Art.º 16.º, n.º 7

A apreensão de dados informáticos, pode, nomeadamente, revestir as formas seguintes:

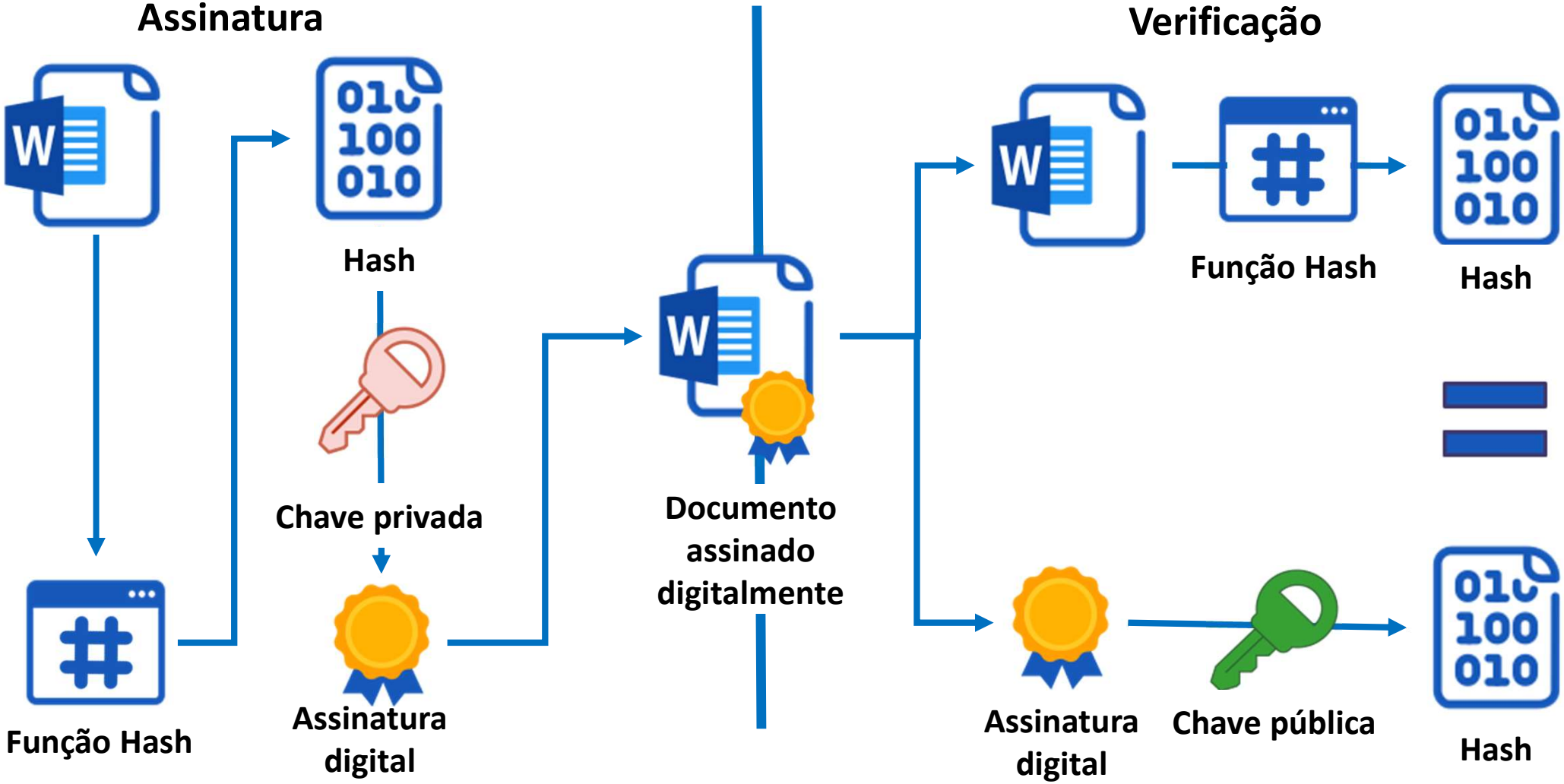
- Apreensão do suporte, bem como dos dispositivos necessários à respetiva leitura;
- Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;
- Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou;
- Eliminação não reversível ou bloqueio do acesso aos dados.

Lei n.º 109/2009

Art.º 16.º, n.º 8

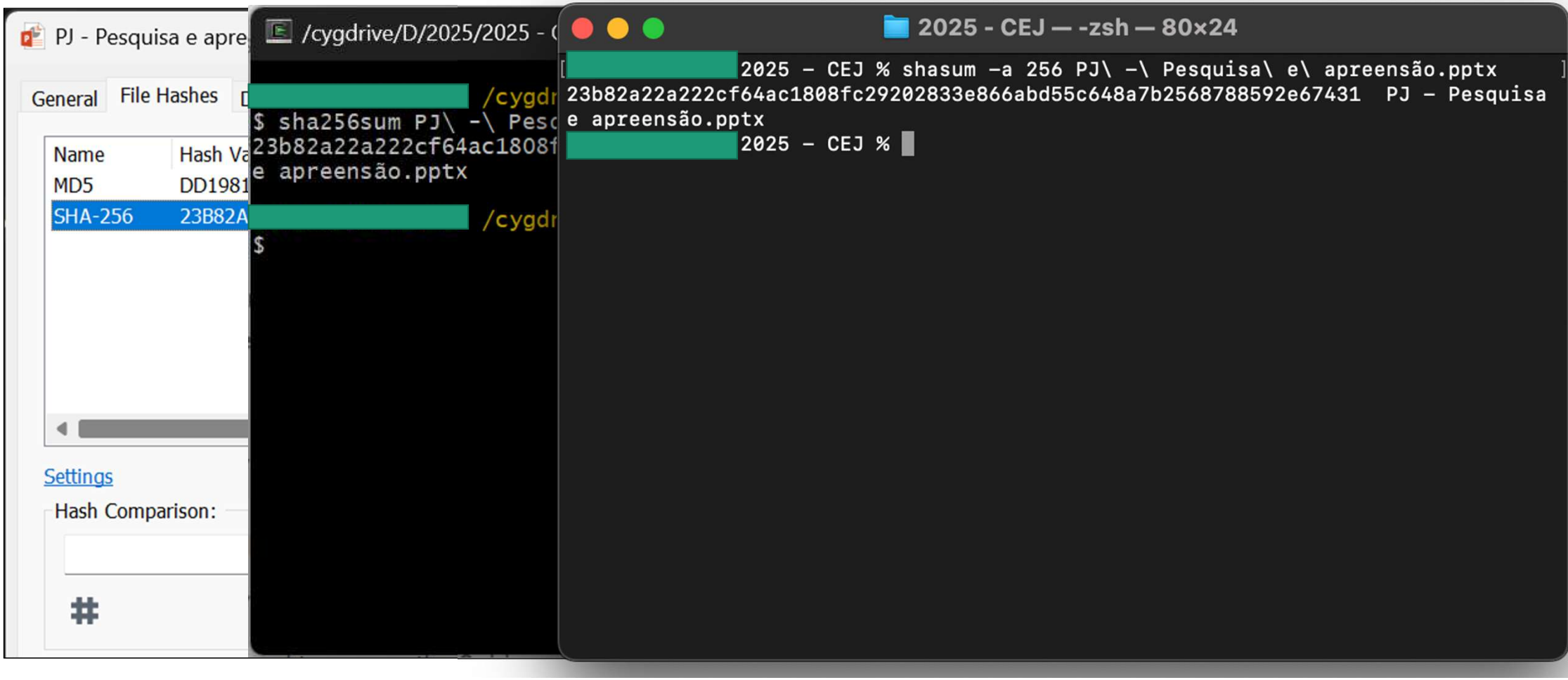
No caso da apreensão efetuada por cópia, esta deverá ser realizada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.

Assinatura Digital



Resumo digital (hash) criptográfico

Funções de hash criptográfico



Funções de hash criptográfico

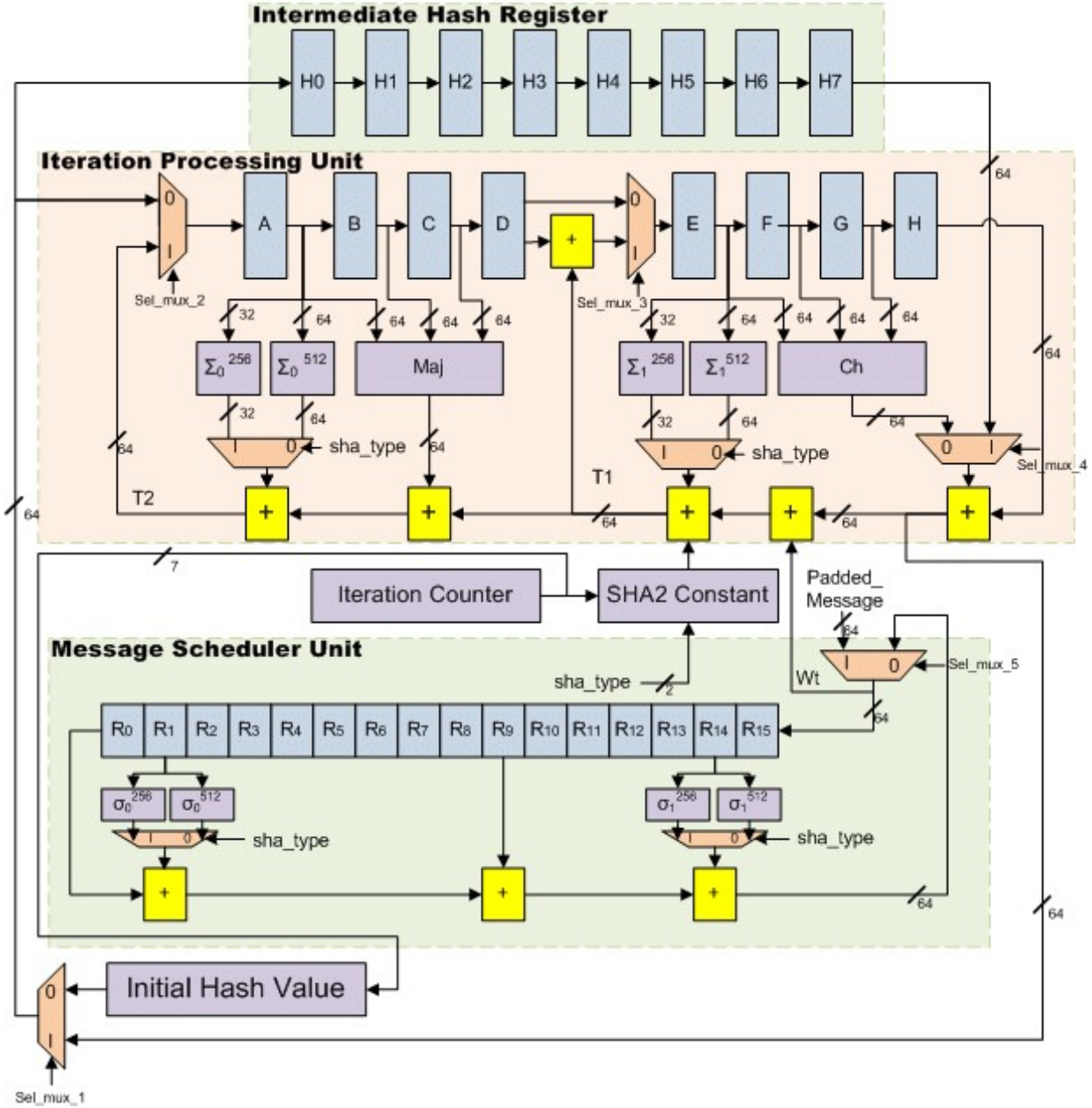
Resumos digitais criptográficos não são cifra. Quando nós ciframos algo, o objetivo é decifrar.

Resumos digitais criptográficos são:

- algoritmos que mapeiam dados de comprimento variável para dados de comprimento fixo
- funções de um sentido único

Um *hash* é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F).

Resumos digitais criptográficos aka *hashes*, *message digests* ou *fingerprints*.


Intermediate Hash Register
H0
H1
H2
H3
H4
H5
H6
H7
Iteration Processing Unit
A
B
C
D
E
F
G
H
Sel_mux_2
Sel_mux_3
Sel_mux_4
Maj
Ch
sha_type
T1
T2
Iteration Counter
SHA2 Constant
Padded_ Message
Wt
Sel_mux_5
Message Scheduler Unit
Initial Hash Value
Sel_mux_1

Acórdão do Tribunal da Relação de Lisboa

1/21.5ICLSB-A.L1-9
FERNANDA SINTRA AMARAL
LEI DO CIBERCRIME
DADOS INFORMÁTICOS
BUSCAS
CÓPIA CEGA
CRIME CONTINUADO

RL
25-01-2024
UNANIMIDADE
S
N

RECURSO PENAL
NÃO PROVIDO

(da responsabilidade da relatora)

I. O legislador da Lei do Cibercrime, com a menção feita no seu art. 15.°, n.°1, à obtenção de dados informáticos específicos e determinados, não pretendeu certamente abarcar uma exigência legal de pré-identificação exacta e rigorosa dos dados informáticos a pesquisar, no decurso de buscas, mas tão-só pretendeu que houvesse uma interligação entre os dados informáticos pesquisados e a sua relevância probatória para a descoberta da verdade material.

II. O procedimento que tem vindo a ser genericamente denominado de "cópia cega", não é, só por si e de forma imediata, reprovável ou inadmissível, podendo encontrar-se justificada a necessidade de se proceder à pesquisa dos dados informáticos (art. 15° da LCC), em local externo, relativamente ao local buscado, por recurso, excepcional, à "cópia cega" de tais ficheiros.

III. É que, a "cópia cega" a que apenas se lançou mão na sequência da grande extensão dos ficheiros a pesquisar, não constitui uma apreensão, em sentido estrito, mas, antes, uma diligência prévia necessária, uma actuação meramente "facilitadora", com vista a permitir um extenso trabalho posterior: a efectivação da pesquisa devida e autorizada pelo JIC - a qual, pela circunstância excepcional referida, deverá ter lugar num local externo.

Acórdão do Tribunal da Relação do Porto

671/14.0GAMCN.P1
JTRP000
MOREIRA RAMOS
LEI DO CIBERCRIME
FACEBOOK
PROVA

RP20170405671/14.0GAMCN.P1
05/04/2017
UNANIMIDADE
S
1

REC PENAL
NEGADO PROVIMENTO
4ª SECÇÃO, (LIVRO DE REGISTO N.º 713, FLS.264-273)
.

I – O Facebook é uma rede social que funciona através da internet, operando no âmbito de um sistema informático pelo que a recolha de prova está sujeita à Lei do Cibercrime - DL 109/2009 de 15/9.
II – Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso.
III – Só esta sujeita à disciplina do art.º 16º 1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível.

Lei n.º 109/2009

Art.º 17.º

Apreensão de correio eletrónico e registos de comunicações de natureza semelhante

A apreensão de correio eletrónico e registos de comunicações de natureza semelhante é da **competência reservada do JIC**.

A autorização ou ordem para a apreensão **tem de ser prévia à sua efetivação**, sob pena de nulidade, conforme disposto no Art.º 179.º, n.º 1 do CPP.

Lei n.º 109/2009

Art.º 17.º

Quando se solicita autorização ao MP para a pesquisa informática, **deve igualmente sugerir-se** que este promova ao JIC a autorização para a apreensão de correio eletrónico e registos de comunicação de natureza semelhante.

Deve respeitar os formalismos do Art.º 179.º do CPP

Acórdão do Tribunal da Relação de Lisboa

165/18.5JASTB.L1-3
CRISTINA ALMEIDA E SOUSA
DADOS INFORMÁTICOS
RECOLHA DE PROVA DIGITAL
AUTORIZAÇÃO

RL
15-07-2020
UNANIMIDADE
S
N

RECURSO PENAL
NEGADO PROVIMENTO

Ainda que possa e deva considerar-se, à semelhança do que é exigido pelo artº174º nº 5 al. c) do CPP que exige o consentimento do visado (e não apenas o de quem tiver a disponibilidade ou controlo dos dados) que só o próprio titular dos direitos postos em crise ou comprimidos com o acesso aos dados informáticos tem legitimidade substantiva e processual para autorizar essa recolha e a sua consideração como provas válidas e eficazes, uma vez prestado o consentimento pelo titular dos dados informáticos, para o acesso e apreensão dos mesmos, para a investigação criminal, fica definitivamente afastada qualquer ilicitude do procedimento de obtenção dessas informações.
Sendo assim, a junção da prova digital pelos órgãos de polícia criminal, no decurso de uma pesquisa informática consentida não carece para ser admissível, válida e eficaz de prévia autorização da autoridade judiciária, independentemente da natureza dos dados obtidos, justamente em face do consentimento previamente prestado pelo titular dos dados, ficando, por essa via, afastada a aplicação dos artigos 16º nºs 1 e 3 e 17º da lei do cibercrime

Lei n.º 109/2009

Art.º 17.º

São consideradas comunicações de natureza semelhante a correio eletrónico as trocadas através de aplicações como WhatsApp, Signal, Telegram, Skype, iMessage, Messenger, etc., independentemente de terem sido lidas ou não.

Também às SMSs se aplica o regime da correspondência, tenham ou não sido lidas.

10 de novembro de 2023

SUPREMO TRIBUNAL DE JUSTIÇA

Acórdão do Supremo Tribunal de Justiça n.º 10/2023

Sumário: «Na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de se encontrarem abertas (lidas) ou fechadas (não lidas), que se afigurem ser de grande interesse para descoberta da verdade ou para a prova, nos termos do art. 17.º, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime)».

Proc. n.º 184/12.5TELSB-R.L1-A.S1

Obrigado!

Contactos:
Francisco Luís – francisco.luis [at] pj.pt
José Amador – jose.amador [at] pj.pt