Prova Digital
no
Crime de Violência Doméstica

Rui Cardoso

Abril | 2022

Sumário:

I. Prova digital – introdução

II. Violência doméstica por meios digitais

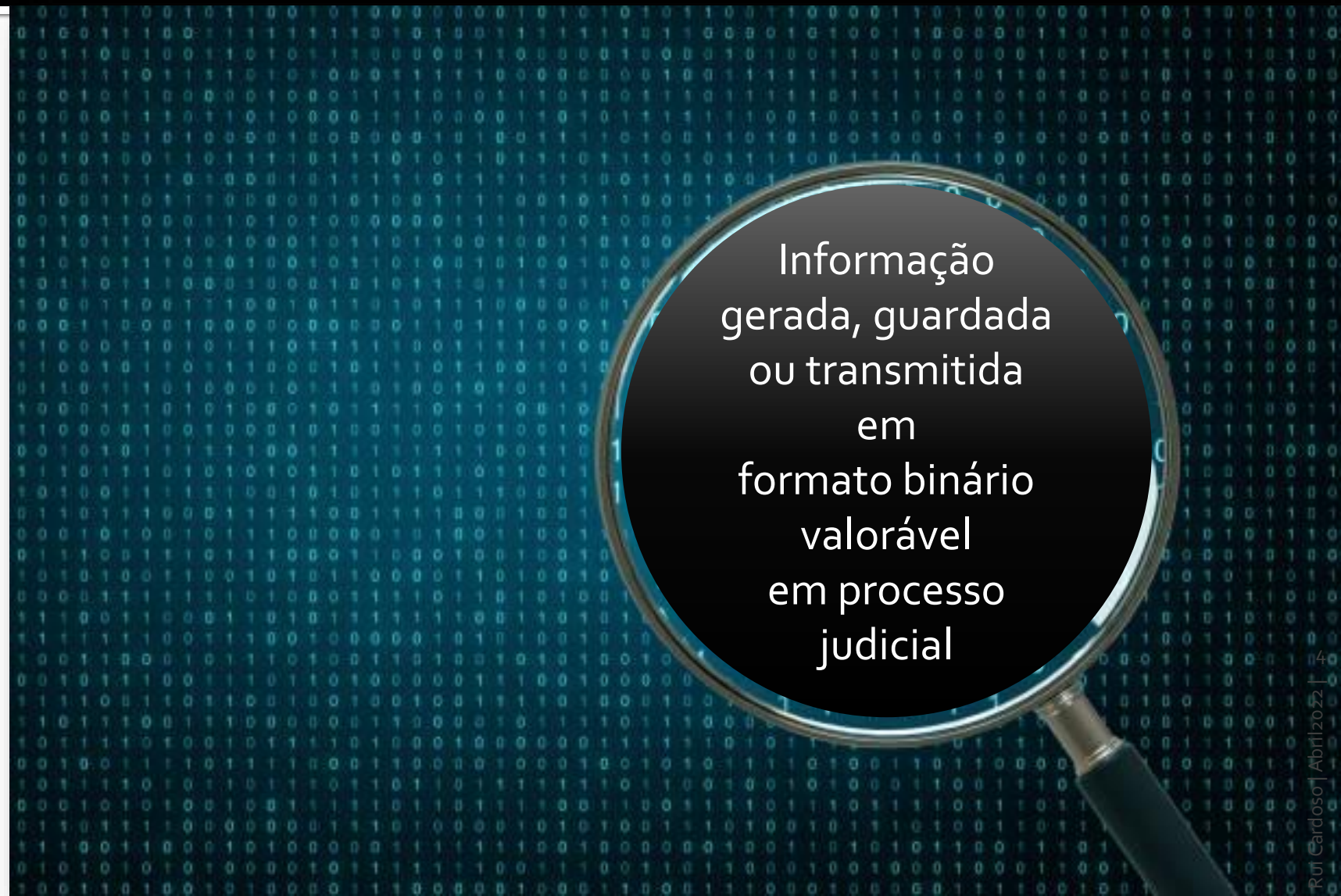
III. Regime geral da prova digital – notas de introdução

IV. Valoração da prova digital

I. Prova digital – introdução

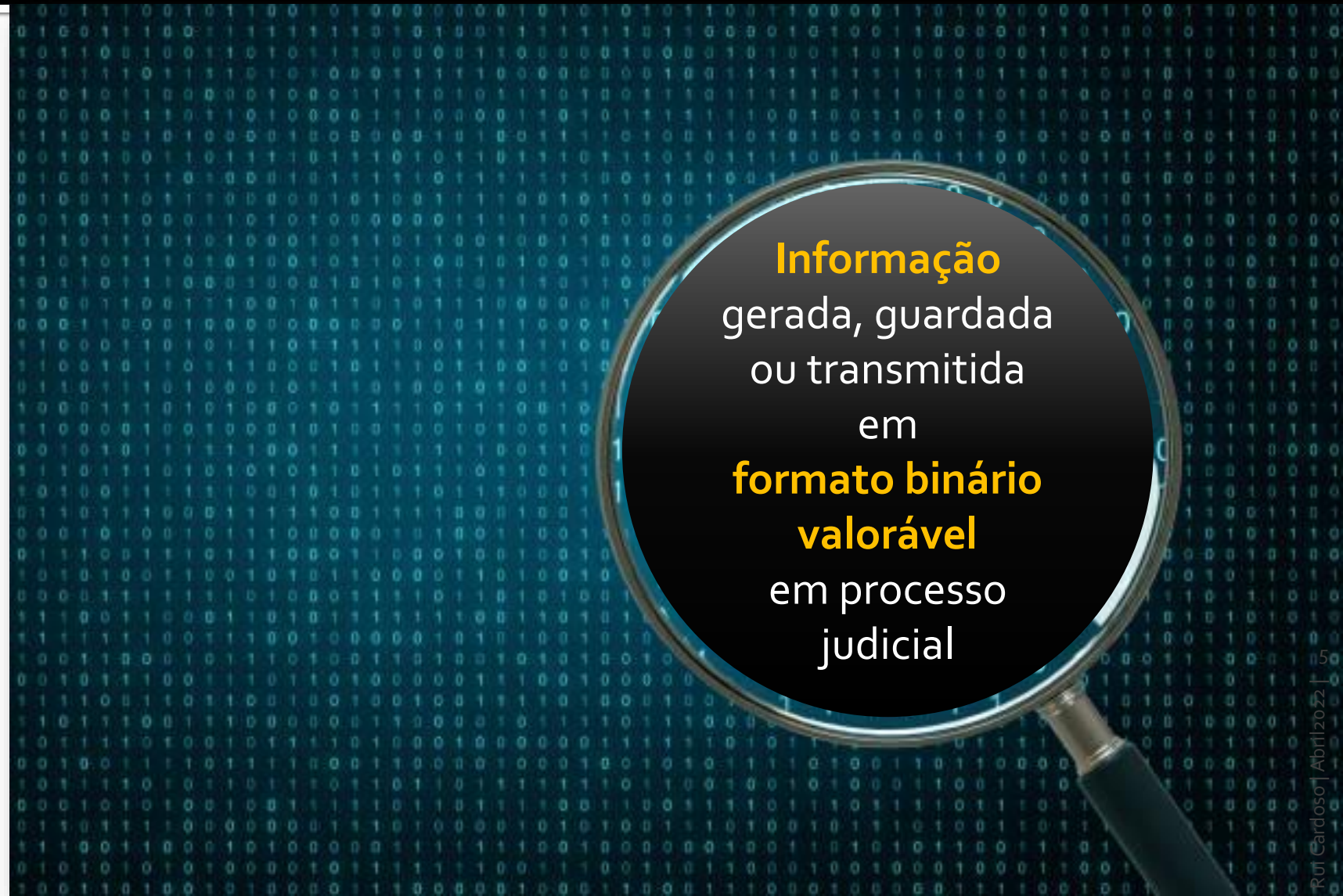
I. Definição

PROVA DIGITAL



I. Definição

PROVA DIGITAL



II. Relevância























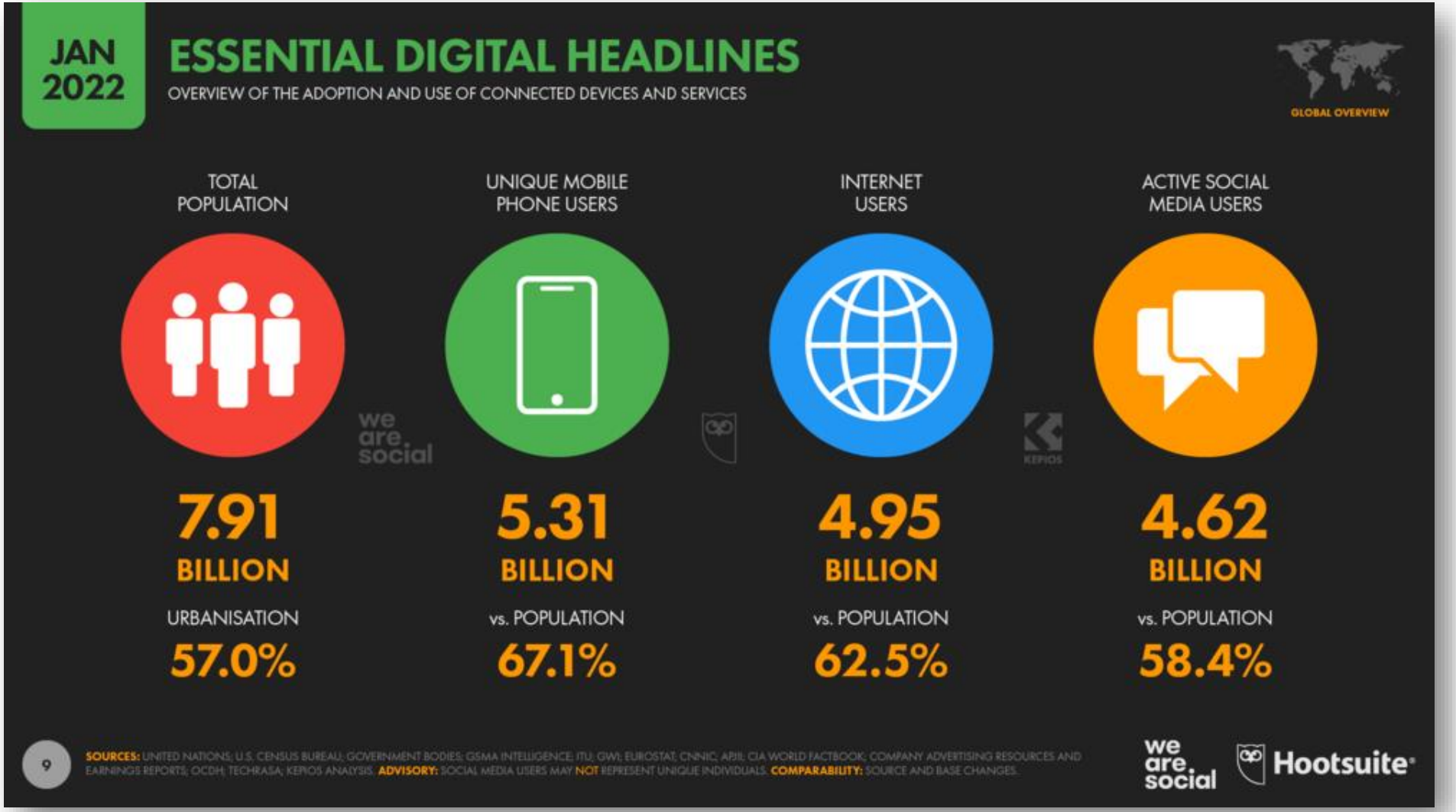




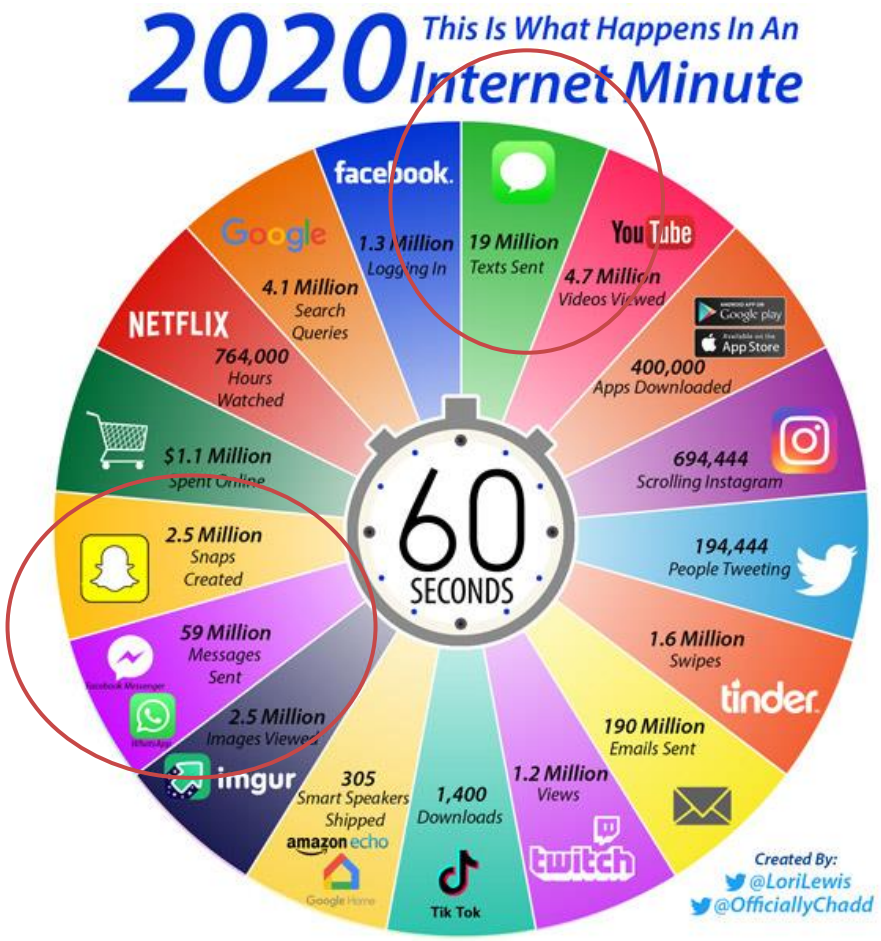


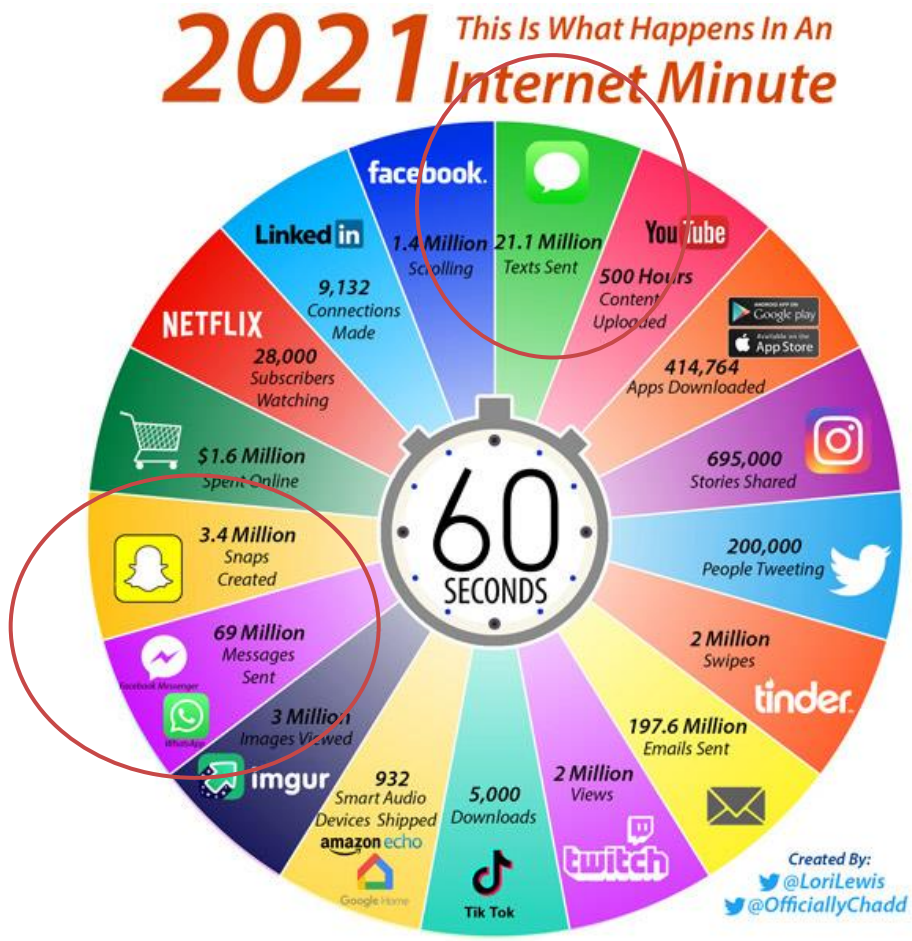

II. Relevância

II. RELEVÂNCIA



II. RELEVÂNCIA





II. Violência doméstica por meios digitais

[Campanha do Governo da Escócia]


STALKERWARE


sms


MMS


REVENGE PORN


EMAIL


DEEP FAKES


I HATE YOU
SEND

III. Regime geral da prova digital

- Notas de introdução

I. Quadro Normativo

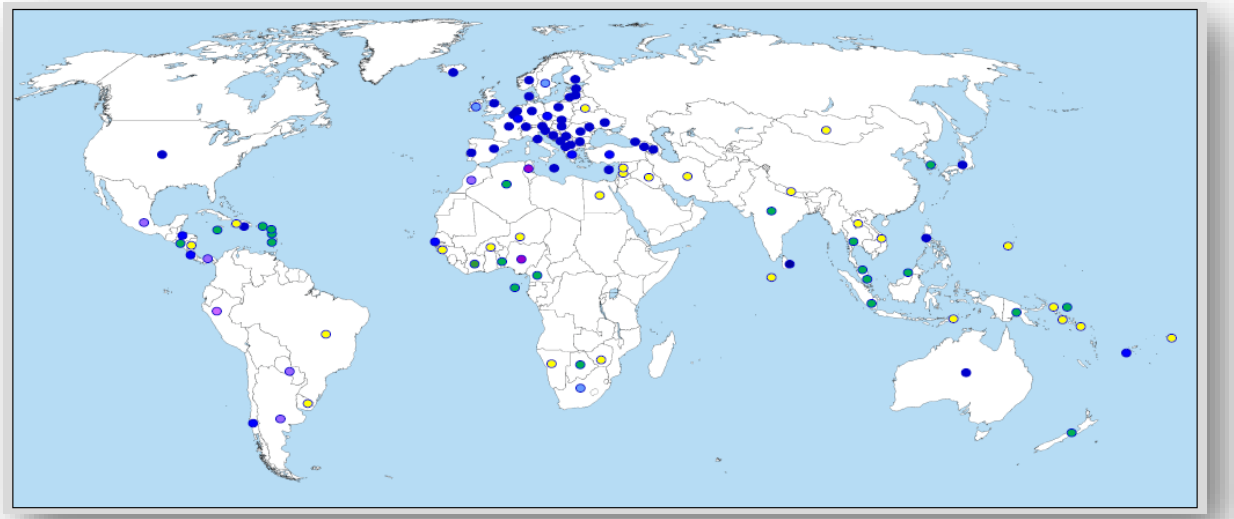
- **Convenção sobre o Cibercrime,** adoptada em Budapeste em 23.11.2001 + 1.º e 2.º Protocolos Adicionais
- **Directiva 2013/40/EU** do Parlamento Europeu e do Conselho de 12.08.2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho
- **Lei 109/2009 (LCC - Lei do Cibercrime)**
- **Lei 32/2008** (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas)
- **Lei 5/2004** (Lei das Comunicações Electrónicas)
- **Lei 7/2004** (Comércio Electrónico no Mercado Interno e Tratamento de Dados)
- **Lei 41/2004** (Tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas)
- **Lei 59/2019** (Lei de Protecção de Dados Pessoais)

I. Quadro Normativo

- **Convenção sobre o Cibercrime**, adoptada em Budapeste em 23.11.2001 + 1.º e 2.º Protocolos Adicionais
- **Directiva 2013/40/EU** do Parlamento Europeu e do Conselho de 12.08.2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho
- **Lei 109/2009 (LCC - Lei do Cibercrime)**
- **Lei 32/2008** (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas)
- **Lei 5/2004** (Lei das Comunicações Electrónicas)
- **Lei 7/2004** (Comércio Electrónico no Mercado Interno e Tratamento de Dados)
- **Lei 41/2004** (Tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas)
- **Lei 59/2019** (Lei de Protecção de Dados Pessoais)

II. Convenção de Budapeste

- 66 países assinaram e ratificaram (45 CoE + 21 não CoE)



- **Explanatory Report!**
- Cybercrime Convention Committee (T-CY) (Guidance Notes)
- Octupus Community (ferramentas sobre cibercrime e prova electrónica)

II. Convenção de Budapeste

- **Direito substantivo** (infracções contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos; infracções relacionadas com computadores; infracções relacionadas com o conteúdo; infracções respeitantes a violações do direito de autor e direitos conexos) **– artigos 2.º a 13.º;**
- **Direito processual**:
  - Artigos 16.º e 17.º - conservação expedita de dados informáticos armazenados
  - Artigo 18.º - injunção de comunicar dados informáticos (ordens de produção)
  - Artigo 19.º - busca e apreensão de dados informáticos armazenados
  - Artigo 20.º - recolha, em tempo real, de dados de tráfego
  - Artigo 21.º - intercepção de dados de conteúdo
  - Artigo 22.º - jurisdição
- **Cooperação internacional (artigos 23.º a 35.º)**
  - Artigo 26.º - informação espontânea
  - Artigos 29.º e 30.º - conservação e revelação expedita de dados informáticos armazenados
  - Artigo 35.º - rede 24/7
  - …

III. LEI DO CIBERCRIME

Artigo 11.º

Âmbito de aplicação das disposições processuais

1 - Com excepção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:

a) Previstos na presente lei;

b) Cometidos por meio de um sistema informático; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

III. Lei do Cibercrime

Artigo 11.º

Âmbito de aplicação das disposições processuais

1 - Com excepção do disposto nos artigos 18.º e 19.º, **as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes**:

a) Previstos na presente lei;

b) **Cometidos por meio de um sistema informático**; ou

c) **Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico**.

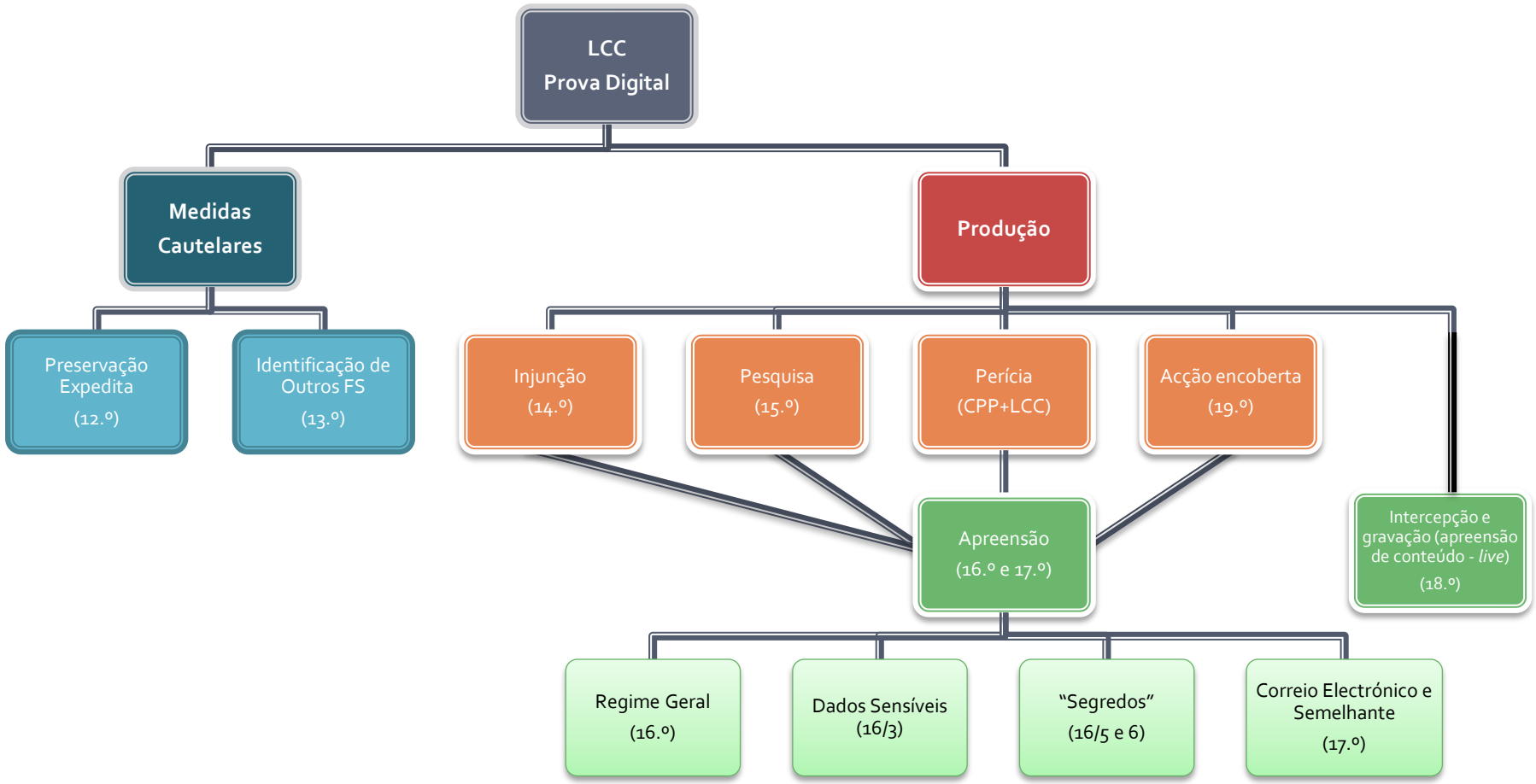
2 - As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

ARTS. 12.º a 17.º - EM ABSTRACTO

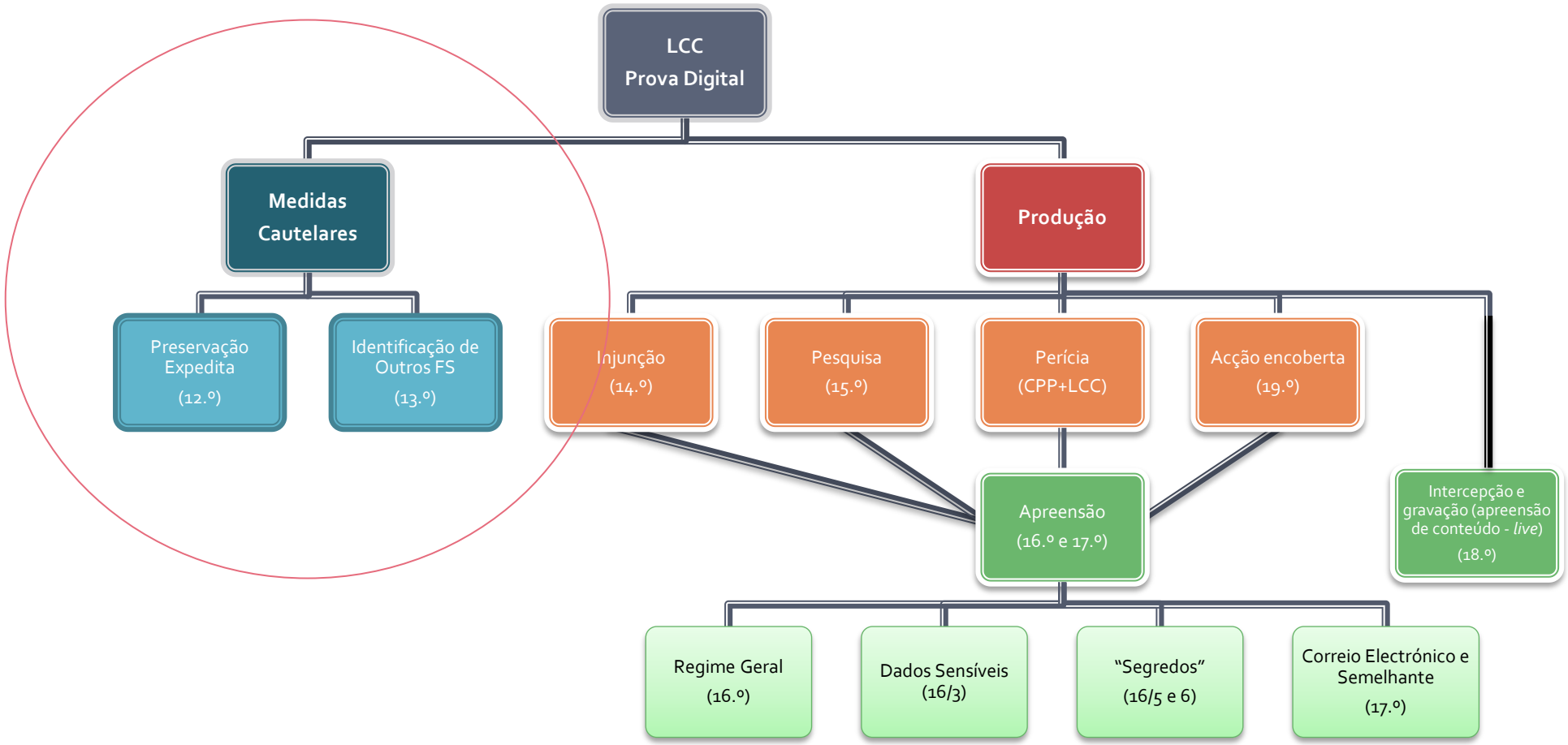
A TODOS OS TIPOS DE CRIME

- REGIME GERAL DE PROVA DIGITAL -

III. Lei do Cibercrime



Medidas Cautelares



A - PRESERVAÇÃO EXPEDITA DE DADOS

B - IDENTIFICAÇÃO DE OUTROS FORNECEDORES DE SERVIÇO

Medidas Cautelares

A. Preservação Expedita de Dados

Artigo 12.º

Preservação expedita de dados

1 - Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.

2 - A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

3 - A ordem de preservação discrimina, sob pena de nulidade:

a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.

MEDIDAS CAUTELARES

A. PRESERVAÇÃO EXPEDITA DE DADOS

4 - Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5 - A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

Medidas Cautelares

A. Preservação Expedita de Dados

- **Finalidade**
  - **Impedir a destruição** de dados informáticos
  - Não é obtenção dos dados!
- **Pressupostos**
  - **Mera necessidade para a prova**, tendo em vista a descoberta da verdade, de
  - Obter **dados informáticos específicos** armazenados num sistema informático, incluindo dados de tráfego
  - **Receio** de que possam perder-se, alterar-se ou deixar de estar disponíveis
- **Competência**
  - Regra: autoridades judiciárias
  - Excepção: OPC's
    - mediante autorização da autoridade judiciária competente ou
    - quando haja urgência ou perigo na demora
      - deverá dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do CPP

Medidas Cautelares

A. Preservação Expedita de Dados

- **Visados**
  - **Qualquer entidade** (designadamente fornecedor de serviço) que tenha disponibilidade ou controlo de dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego

- **Duração**
  - Período fixado, que **não pode ultrapassar 3 meses**
  - **Renovações** – cada uma não pode ultrapassar 3 meses e no total não podem ultrapassar 1 ano

- **Formalismos**
  - **Despacho fundamentado**, com ordem de preservação, que, sob pena de nulidade, deve discriminar:
    - A **natureza** dos dados;
    - A sua **origem e destino**, se forem conhecidos; e
    - O **período** de tempo pelo qual deverão ser preservados, até um máximo de 3 meses.
  - **Ofício** dirigido à entidade visada

MEDIDAS CAUTELARES
B. IDENTIFICAÇÃO DE OUTROS FORNECEDORES DE SERVIÇO

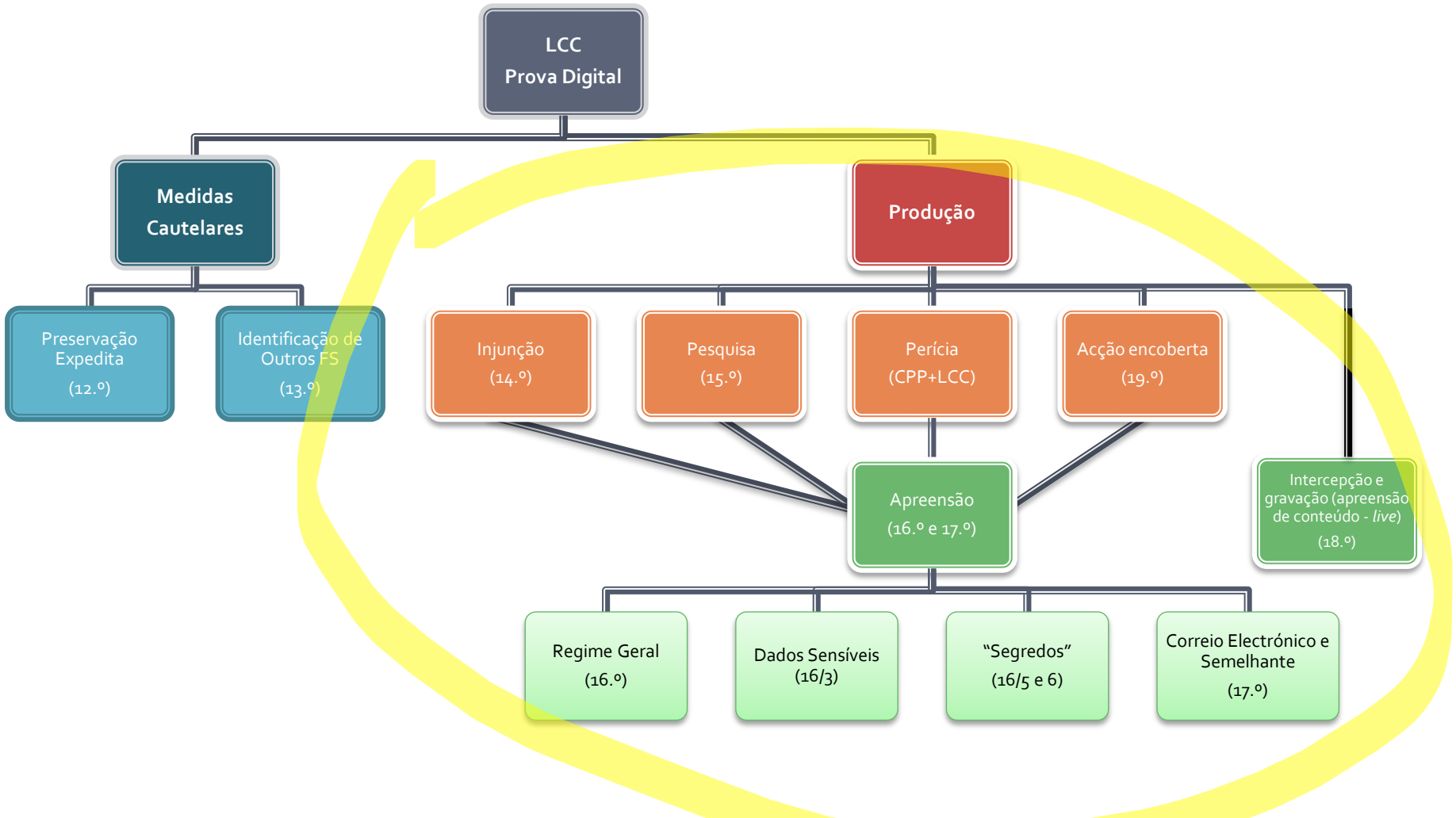
Artigo 13.º

Revelação expedita de dados de tráfego

Tendo em vista assegurar a **preservação** dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

- **Não é revelação de dados de tráfego**
- Apenas **obrigação** (*ope legis*) para o **fornecedor de serviço** a quem tenha sido ordenada a preservação de dados de…
- **… indicar** a quem ordenou a preservação (AJ ou OPC) que **há outros fornecedores de serviço** através dos quais aquela comunicação tenha sido efectuada
- **Para permitir que também a esses seja dada ordem de preservação de dados**

Produção de Prova Digital



Produção de Prova Digital

- **Dados armazenados:**
  1. **Dados em suporte <u>na posse de outras entidades</u>**
     - injunção para **apresentação** dos dados → apresentação → apreensão
     - injunção para **concessão de acesso** aos dados → pesquisa → apreensão
  2. **Dados em suporte <u>na posse das AJ/OPC</u> ou acessíveis através desse suporte**
     - pesquisa/perícia → apreensão

- **Dados em trânsito:**
  1. **Intercepção** → gravação

A apreensão de dados é, verdadeiramente, uma decisão de *utilizabilidade* probatória, não a aquisição da posse física dos dados (como sucede com as apreensões de coisas)

Produção de Prova Digital

A. Injunção para Apresentação ou Concessão do Acesso a Dados

Regime Geral

"Mera" necessidade

Artigo 14.º

Injunção para apresentação ou concessão do acesso a dados

INQ = MP

1 - Se no decurso do processo se tornar **necessário à produ** tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num **determinado sistema informático**, a **autoridade judiciária competente** ordena disponibilidade ou controlo desses dados que os comunique ao processo ou que p

189/2 CPP - 187/1
Lei 32/2008 - crimes graves
JI

Não é só para telecomunicações!

e punição por desobediê

Dados de base

4 - O disposto no presente artigo é aplicável a **necedores de serviço**, a quem ser ordenado que comuniquem ao processo **dados relativos aos seus clientes ou assinantes, neles e incluindo qualquer informação** diferente dos dados relativos ao tráfego ou ao conteúdo, formáticos ou sob qualquer outra forma, detida pelo fornecedor minar:

Regime Especial Fornecedores de Serviço

Intercepção

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

IP

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e **qualquer outro número de acesso**, os **dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços**; ou

c) Qualquer outra informação sobre a **localização** do equipamento de comunicação, **disponível com base num contrato ou acordo de serviços**.

Produção de Prova Digital

A. Injunção para Apresentação ou Concessão do Acesso a Dados

5 - A injunção prevista no presente artigo **não pode ser dirigida a <u>suspeito ou arguido</u>** nesse processo.

6 - Não pode igualmente fazer-se uso da injunção prevista ne[illegible] informáticos utilizados para o exercício da **advocacia,** das actividades **médica** e **bancária** e da profissão de **jornalista**.

7 - O regime de **segredo profissional** ou de **funcionário** e de segredo **de Estado** prev[illegible]o artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Busca/revista para apreensão do suporte -» pesquisa -» apreensão dados

Regime de quebra do segredo

Excluir - interpretação actualista. A Lei 36/2010 alterou o RJICSF no sentido de excepcionar do regime de segredo bancário o fornecimento de elementos às autoridades judiciárias, afastando a aplicação do regime geral de segredo profissional constante do art. 135/3 do CPP

Artigo 15.º

Pesquisa de dados informáticos

1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

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

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

a) 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;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

5 - Quando, no decurso de pesquisa, surgirem razões para crer que **os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado**, mas que tais dados são **legitimamente acessíveis a partir do sistema inicial**, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.ºs 1 e 2.

6 - À pesquisa a que se refere este artigo **são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.**

- **Finalidade**
  - **Obter dados informáticos específicos e determinados,** armazenados num determinado sistema informático

≠

de **apenas ver** dados específicos e determinados!
Como numa **busca**
(identificação prévia, tão precisa quanto possível, sobre o que se pretende)

Se estiverem em trânsito → **intercepção**

- **Finalidade**
  - **Obter dados informáticos específicos** e **determinados**, armazenados num determinado sistema informático
- **Necessidade**
  - O artigo 15/1 não contém qualquer exigência reforçada quanto à necessidade para a prova (apenas "tendo em vista a descoberta da verdade") – **mera necessidade**
  - Porém, face aos direitos fundamentais que no caso podem ser ofendidos – privacidade/intimidade, autodeterminação informacional, inviolabilidade de comunicações(?) –, há que aplicar a regra geral decorrente do artigo 18/2 CRP: **necessidade, adequação, proporcionalidade em sentido estrito**
    - A mera execução da pesquisa e o conhecimento que dela advirá já poderão ser ofensa a esses direitos fundamentais, mesmo que nenhuma apreensão de dados venha a ocorrer
    - Assim, quanto maior a previsível ofensa, maior deve ser a exigência quanto à necessidade e proporcionalidade
  - Também não se exige qualquer particular grau prévio de indícios sobre os crimes para cuja prova a pesquisa servirá

- **Âmbito**
  - **Catálogo de crimes**
    - Não existe – artigo 11.º, n.º 2, LCC (em abstracto, qualquer tipo de crime em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico)
  - **Pessoas visadas**
    - Catálogo do artigo 187/4 CPP (escutas)?
      - Sim (Duarte Nunes)
    - Quaisquer pessoas
      - Pelos mesmos fundamentos que não existe para as buscas (os dados a apreender podem estar na posse/disponibilidade de quaisquer pessoas, mesmo de boa fé)
        - » Claro que, quanto "mais longe" estivermos do arguido, maiores serão as exigências de proporcionalidade – tal como numa busca
      - Os dados até podem estar em sistemas informáticos sem ligação a qualquer pessoa determinada ou determinável e/ou não conter dados pessoais
  - **Fase do processo**
    - Inquérito, instrução ou julgamento

- **Sistemas informáticos**
  - Sistema informático **determinado**, onde estão armazenados **dados informáticos específicos e determinados**
    - Deve ser individualizado com a precisão possível, v. g., pelo local onde se encontra (p. ex., todos os sistemas informáticos que forem encontrados no local A, onde se indicia que as notas são contrafeitas), pelo seu utilizador (p. ex., todos os sistemas informáticos que forem encontrados na posse do suspeito/arguido X), pela sua função (p. ex., o servidor da pessoa colectiva arguida Y utilizado para o backup do correio electrónico)
    - Mas não é necessário estar identificado por marca, modelo, MAC, IMEI, etc.
  - **Outro sistema informático**, ou parte diferente do sistema pesquisado, onde os dados pretendidos possam estar, desde que (n.º 5):
    - seja possível o **acesso legítimo** a partir do sistema inicial
      - acesso legítimo (oposto do acesso ilegítimo previsto no artigo 6/1: ou acesso do proprietário, ou com permissão legal, ou com autorização do proprietário ou de outro titular do direito do sistema)
    - haja **autorização ou ordem da autoridade competente**
      - pode ser dada no despacho inicial, se a AJ não pretender presidir
      - **exemplos**: *clouds*, servidores de correio electrónico, redes sociais

- **Competência**
  - **Regra**: **autoridades judiciárias**
    - No **inquérito,** o Ministério Público
      - Não há inconstitucionalidade
        - » Só há reserva de juiz para os meios de obtenção de prova com restrições intensas de direitos fundamentais
        - » Na pesquisa pode não haver qualquer restrição
        - » Quando há restrição mais intensa, a utilização processual depende de decisão judicial (artigos 16/3 e 17)
        - » Assim: Paulo Pinto de Albuquerque, Tiago C. Milheiro e Duarte R. Nunes; contra TC 687/2021?
      - Excepção: os regimes especiais de protecção de segredos previstos no CPP (em que, para as buscas, a competência para ordenar é expressamente do juiz de instrução, que depois a elas deve presidir)
    - Ministério Público ou juiz de instrução conforme o local onde se encontra o sistema?
      - Confunde acesso ao local físico onde está o sistema e acesso aos dados informáticos (fazendo depender a protecção a estes de factores completamente aleatórios)
    - Na **instrução e julgamento**
      - O juiz

- **Competência**
  - **Regra**: **autoridades judiciárias**

    - **Despacho fundamentado** (nos termos gerais)
      → mandado de pesquisa e apreensão de dados informáticos

    - Deve ser fixada uma **validade máxima**
      - não pode exceder 30 dias (mas pode ser menor)

    - Sempre que possível, a AJ deve **presidir à pesquisa**
      - Quando preveja que tal não lhe seja possível, deve desde logo justificar no despacho essa impossibilidade

- **Competência**
  - **Excepção**: **OPC's, sem prévia autorização da autoridade judiciária, quando (n.º 3):**

  a) A mesma for **voluntariamente consentida** por **quem tiver a disponibilidade ou controlo** desses dados, desde que o consentimento prestado fique, por qualquer forma, **documentado**;

    - Diferente do disposto no artigo 174/5 b) ("visados"), mas igual à interpretação que desse artigo deve ser feita
      - O consentimento terá de ser **apenas de quem seja titular dos direitos (eventualmente) ofendidos com a pesquisa**

    - **"disponibilidade ou controlo":**
      - **Disponibilidade** – posse física dos dados, com possibilidade de acesso imediato;
      - **Controlo** – ausência de posse física, mas possibilidade de acesso remoto com domínio sobre a sua produção (e não apenas de acesso ou consulta).
        - Cfr. parágrafo 173 do Relatório Explicativo da CCiber: "[a] expressão "posse ou controlo" refere-se à posse física dos dados em questão no seio do território da Parte que emite a ordem, bem como a situações em que os dados a serem produzidos não se encontram na posse física da pessoa mas sendo possível, contudo, a esta última exercer livremente o seu controlo sobre a produção dos dados a partir do território da Parte emissora da ordem".

- **Competência**
  - **Excepção**: **OPC's, sem prévia autorização da autoridade judiciária, quando (n.º 3):**

    - **Consentimento** deve ser
      - **Esclarecido** (não pode ser obtido de forma enganosa; pessoa tem de perceber o que está em causa (aquilo com que concorda) e que não está obrigada a concordar)
      - **Prévio** (antes da pesquisa)
      - **Expresso** (não pode ser tácito) e
      - **Documentado** (documento assinado, gravação áudio ou áudio e vídeo)

    b) Nos casos de **terrorismo, criminalidade violenta ou altamente organizada**, quando **haja fundados indícios da prática iminente de crime** que ponha em **grave risco a vida ou a integridade de qualquer pessoa.**
      - Igual ao artigo 174/5 a) CPP
      - Terrorismo, criminalidade violenta ou altamente organizada – artigo 1.º, alíneas i), j) e m)

- **Competência**
  - **Excepção: Autoridades de Polícia Criminal da Polícia Judiciária**

    - Podem ordenar a realização de pesquisa em sistema informático **sempre que não seja possível, dada a situação de urgência e perigo na demora, aguardar pela decisão de autoridade judiciária** – artigo 9/1 f) da NLOPJ (DL 137/2019)
      - Não necessitam despacho da autoridade judiciária
      - Deve haver urgência e perigo na demora que imponha que não se possa aguardar pela decisão de AJ
      - Deve haver despacho fundamentado da APC
      - A execução deve ser imediata (se não for, há que recorrer à AJ)

    - "A realização desse actos obedece à tramitação do CPP e tem de ser de imediato comunicada à autoridade judiciária titular da direção do processo para os efeitos e sob as cominações da lei processual penal" – artigo 9/2 NLOPJ
      - Quanto à pesquisa informática, as referências ao CPP devem ser entendidas como feitas à LCC

- **Formalismos Código de Processo Penal** (por força do artigo 15/6 LCC - *À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal*)

  - **Comunicações ao visado e presença na pesquisa** – artigo 176.º CPP

    1 - Antes de se proceder a busca, é **entregue** (…) a quem tiver a disponibilidade do lugar em que a diligência se realiza, **cópia do despacho que a determinou,** na qual se faz menção de que **pode assistir à diligência** e **fazer-se acompanhar ou substituir por pessoa da sua confiança e que se apresente sem delonga**.

    2 - Faltando as pessoas referidas no número anterior, a cópia é, sempre que possível, entregue a um parente, a um vizinho, ao porteiro ou a alguém que o substitua.

Pode ser advogado, técnico de informática ou outra pessoa qualquer

PERÍCIA INFORMÁTICA FORENSE / PERÍCIA DIGITAL FORENSE / ANÁLISE FORENSE

- **O que é: inspecção sistemática e tecnológica de um sistema informático e/ou dos seus conteúdos para a obtenção de provas de um crime** ("quê", "quem", "quando", "como", "onde", "porquê");
- **Finalidade: encontrar dados, apreendê-los** e **analisá-los**

- **Regime Legal**:
  - **CPP** (artigos 151.º - 163.º)
  - **LCC** apenas quanto à apreensão de dados pessoais ou íntimos, de segredos profissionais, de correio electrónico e registos de comunicações de natureza semelhante (artigos 16, n.ºs 3, 5 e 6, e 17.º) – **competências do JIC**
    - não quanto ao prazo de validade do despacho

- Pode ser feita sobre **dados ainda não apreendidos** ou sobre **dados já apreendidos**

Artigo 16.º

Apreensão de dados informáticos

1 - Quando, 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.

2 - O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3 - Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo 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.

4 - As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5 - As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista.

6 - O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações

Notas gerais

7 - A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

d) Eliminação não reversível ou bloqueio do acesso aos dados.

8 - No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada 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.

REGIMES

1. **Artigo 16/1 e 2 –** Regime geral

ESPECIAIS

2. **Artigo 16/3 – "Dados pessoais ou íntimos"**
3. **Artigo 16/5** – Sistemas informáticos utilizados para o exercício da **advocacia** e das actividades **médica** e **bancária** (aplica-se, com as necessárias adaptações, às regras e formalidades previstas nos artigos 180.º e 181.º CPP), sistemas informáticos utilizados para o exercício da profissão de **jornalista** (aplica-se, com as necessárias adaptações, as regras e formalidades previstas no Estatuto do Jornalista)
4. **Artigo 16/6** – O regime de **segredo profissional** ou de **funcionário** e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.
5. **Artigo 17.º** – **Mensagens de correio electrónico** ou registos de comunicações de natureza **semelhante**

DADOS INFORMÁTICOS

- **O que pode ser apreendido**
  - dados ou documentos informáticos
  - necessários à produção de prova, tendo em vista a descoberta da verdade

O artigo 16/1 não contém qualquer exigência reforçada quanto à necessidade para a prova (apenas "tendo em vista a descoberta da verdade") – *mera necessidade*

Porém, face aos **direitos fundamentais** que no caso podem ser ofendidos (privacidade/intimidade, autodeterminação informacional, inviolabilidade de comunicações?), há que aplicar a regra geral decorrente do artigo 18/2 CRP: **necessidade, adequação, proporcionalidade em sentido estrito**

Como já são conhecidos os dados a apreender (o que não acontecia com a pesquisa), este juízo de ponderação é já totalmente **concreto**

DADOS INFORMÁTICOS

- **O que pode ser apreendido**
  - dados ou documentos informáticos
  - necessários à produção de prova, tendo em vista a descoberta da verdade

- **Modo de obtenção**
  - Durante uma **pesquisa informática legítima**
    - **Nota:** pesquisa do artigo 15/5 ainda é pesquisa
  - Durante **outro acesso legítimo** (perícia informática/análise forense)

ÂMBITO

- Catálogo de crimes
  - Não existe – artigo 11.º, n.º 2, LCC
- Pessoas visadas
  - Catálogo do artigo 187/4 CPP (escutas)?
    - Sim (Duarte Nunes)
  - **Quaisquer pessoas**
    - Os dados podem respeitar a quaisquer pessoas (os dados a apreender podem estar na posse/disponibilidade de quaisquer pessoas, mesmo de boa fé)
      - Claro que, quanto "mais longe" estivermos do arguido, maiores serão as exigências de proporcionalidade
    - Os dados podem até não ter qualquer ligação a pessoa determinada ou determinável e/ou não conter dados pessoais
- Fase do processo
  - Inquérito, instrução ou julgamento

COMPETÊNCIA

- **Regra**: **autoridades judiciárias**
  - Inquérito – Ministério Público
  - Instrução e Julgamento – Juiz

  } Despacho fundamentado

- **Excepção**: **OPC's por iniciativa própria**:
  - No decurso de **pesquisa informática** legitimamente ordenada e executada, ou seja:
    - **voluntariamente consentida** por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
    - casos de **terrorismo, criminalidade violenta ou altamente organizada**, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa;
  - Quando haja **urgência ou perigo na demora**;
    - Como é que têm acesso aos dados? Nesses casos, podem afinal fazer pesquisas?

Validação

VALIDAÇÃO

- As apreensões efectuadas por OPC (em cumprimento de mandado ou por iniciativa própria) **são sempre sujeitas a validação pela AJ,** no prazo máximo de **72 horas**:
  - Inquérito – Ministério Público
  - Instrução e Julgamento – Juiz

- **Incumprimento?**
  - Falta de validação da **pesquisa** não autorizada (mas em que se verificam os fundamentos do artigo 15/3) – **nulidade** (expressamente prevista - 15/4a)
  - Falta de validação da **apreensão** – **irregularidade**
- Fundamento da diferença?
  - A violação da privacidade já ocorreu com a pesquisa, o acto formal de apreensão é menos grave
  - Igual a CPP

MODOS DE APREENSÃO

N.º 7: A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

1. **Apreensão do suporte** onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;
2. Realização de **cópia dos dados**, em duplicado, em suportes autónomos;
   - Uma das cópias será junta ao processo e a outra será selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos;
     - suportes "esterilizados" (*checksum* = 0)
   - Se tal for tecnicamente possível, os dados apreendidos são certificados por meio de **assinatura digital**;
     - Assinatura digital – certificação de que a cópia é igual ao original
     - *Hashing - é um método de representação de uma colecção de dados através de um número único, que resulta da aplicação de um algoritmo matemático a esses mesmos dados. Dois ficheiros com exactamente a mesma sequência de bits, devem produzir o mesmo código hash quando se utiliza o mesmo algoritmo.*

3. **Preservação, por meios tecnológicos, da integridade dos dados**, sem realização de cópia nem remoção dos mesmos;

   ou

4. **Eliminação não reversível** ou **bloqueio do acesso aos dados**.

– **3 e 4 não são verdadeiras apreensões**, pois se não se lhes seguir umas das apreensões 1 ou 2 não há forma de utilizar tais dados como prova

– **Critérios para a escolha** (tendo em conta os interesses do caso concreto)

- **Adequação**
- **Proporcionalidade**

} de todos os meios <u>adequados</u>, deverá ser utilizado o <u>menos lesivo</u> para o visado

  – NB - visado não poderá ficar com acesso aos dados se a mera posse for proibida (exemplos: pornografia infantil, reproduções ilegítimas de programas protegidos, programas destinados a intercepções de comunicações, acesso ilegítimo a sistemas, a dano ou sabotagem, *etc*.)

3 - Caso sejam apreendidos dados ou documentos informáticos **cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo 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.

- **Aplica-se a:**
  - dados ou documentos informáticos **já apreendidos**
  - cujo conteúdo seja susceptível de revelar **dados pessoais ou íntimos,** que possam pôr em causa a **privacidade do respectivo titular ou de terceiro**
    - Dados **íntimos** – por regra, estará sempre em causa a privacidade do titular ou terceiro (sempre aplicação do 16/3)
    - Dados **pessoais** – apenas os dados sensíveis, como diários, dados de saúde, de práticas religiosas, etc. (excluindo dados pessoais como nome, morada, números de cartões de identificação, número de telefone, e-mail, e quaisquer dados que sejam do conhecimento público, v. g., em redes sociais)

3 - Caso sejam apreendidos dados ou documentos informáticos **cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo 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.

- **Formalismo:**
  - os dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto;
    - suporte autónomo só com esses dados
    - MP é que apresentará, justificando o seu relevo probatório

- **Necessidade**:
  - O 16/3 não apresenta qualquer real critério ("interesses do caso concreto"?), mas exige-se **reforçadas necessidade, adequação e proporcionalidade** (18/2 CRP)

- **As apreensões relativas a sistemas informáticos utilizados para:**
  - exercício da **advocacia** e da **actividade médica** estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 180.º CPP;
  - exercício da **actividade bancária** está sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 181.º CPP;
  - exercício da profissão de **jornalista** estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista (artigo 11.º da 64/2007)
- O regime de **segredo profissional** ou de **funcionário** e de **segredo de Estado** previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Por força dessas remissões,

exige-se intervenção prévia do juiz de instrução

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma **pesquisa informática** ou **outro acesso legítimo** a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja pe[illegible] partir do primeiro, mensagens de correio electrónico c[illegible]es de natureza semelhante, o juiz pode autorizar ou or[illegible]ensão daque[illegible] de grande interesse para a descoberta da verdade ou para[illegible] correspondentemente o regime da apreensão de corres[illegible] Código de Processo Penal.

Perícias, se estas forem realizadas antes da apreensão

Acesso aos dados que estejam na disponibilidade ou controlo de outra entidade, por esta concedido, previsto no n.º 1 do artigo 14.º

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático **ou noutro a que seja permitido o acesso legítimo a partir do primeiro**, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

v. g., servidores de correio electrónico

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, **mensagens de correio electrónico** ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descob para a prova, aplicando-se correspondentemente o regime d rrespondê Código de Processo Penal.

internet

intranet

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou **registos de comunicações de natureza semelhante**, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Apenas dados de tráfego de outras transmissões electrónicas de mensagens?

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de **comunicações de natureza semelhante**, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Através de serviço telefónico – *SMS, EMS, MMS*

Número telefónico

Através da *internet* ou *intranets* - *Instant messengers, chats/chatrooms*, ...?

IP

Âmbito de aplicação do artigo 17.º da LCC

- **Distinção entre mensagens abertas e não abertas / lido e não lido?**
- **Distinção entre mensagens que estão nos servidores dos ISP e mensagens já descarregadas para os sistemas informáticos dos seus destinatários?**
- **Artigo 17.º aplica-se mesmo se existir consentimento de quem tem a disponibilidade ou controlo dos dados?**

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, **o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova**, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no

Só a partir desse momento há formalmente a apreensão (possibilidade de utilização/valoração). Mas já existia apreensão nos termos do artigo 16/7a ou b… (apreensão cautelar ou provisória)

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, **o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova**, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Artigo 17.º

Apreensão de correio electrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, **o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal**.

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

- **O artigo 17.º determina a *correspondente* aplicação do regime de apreensão de correspondência do CPP, *não a aplicação integral*.**

- Esta só deve ser feita **naquilo que não contrariar o já previsto na própria LCC** – a remissão para o CPP não pode sobrepor-se ao regime especial de prova electrónica previsto na LCC:

  - O artigo 17.º da LCC não tem previsão sobre **invalidades**, pelo que deve operar a remissão para o CPP, aplicando-se o regime do artigo 179.º;

  - O artigo 17.º da LCC não tem previsão sobre a apreensão de correspondência electrónica ou semelhante **entre o arguido e o seu defensor**, pelo que deve operar a remissão para o CPP (só será admissível se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime);

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

- **O artigo 17.º determina a *correspondente* aplicação do regime de apreensão** *[illegible]a aplicação integral*.
- **[illegible]não contrariar o já previsto na própria LCC** – a [illegible] sobrepor-se ao regime especial de prova

Proibição de prova (126/3)

1. apreensão sem autorização judicial
2. apreensão de correspondência entre o arguido e o seu defensor, sem que o juiz tenha fundadas razões para crer que aquela constitui objecto ou elemento de um crime
3. valoração de correspondência não apreendida

Irregularidade

1. omissão do exame pelo juiz
2. …

[illegible]visão sobre **invalidades**, pelo que deve operar a [illegible] artigo 179.º;

[illegible]ão sobre a apreensão de correspondência [illegible]**guido e o seu defensor**, pelo que deve operar a [illegible]sível se o juiz tiver fundadas razões para crer que [illegible]to de um crime);

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Notas de comparação CPP - LCC

CPP – 179.º		LCC – 17.º
Aplica-se a correspondência **em trânsito ou ainda não aberta**	≠	Não há verdadeiramente regime de aberto/fechado
Catálogo (estar em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos)	≠	O artigo 17.º **não tem catálogo** (artigo 11/1)
A correspondência tem de ser expedida pelo **suspeito** ou lhe ser dirigida	≠	Pode respeitar a **qualquer pessoa**
Critério de necessidade – grande interesse para a descoberta da verdade ou para a prova	=	**Critério de necessidade** – grande interesse para a descoberta da verdade ou para a prova

A diferença não é significativa, pois, no corpóreo:

- a correspondência do suspeito/arguido, depois de recebida, pode ser apreendida na posse de qualquer pessoa (mero documento);
- a correspondência remetida/dirigida a não suspeito/arguido pode vir a ser apreendida depois de recebida (mero documento);

A importância é elevada:

- *v. g.*, no âmbito da criminalidade dos entes colectivos, em que a correspondência electrónica de grande interesse probatório pode ser trocada por pessoas humanas não suspeitos/arguidos, normalmente de boa fé, no interior dessas organizações;

Única interpretação conforme ao artigo 14.º da CCiber

A correspondência tem de ser expedida pelo **suspeito** ou lhe ser dirigida	≠	Pode respeitar a **qualquer pessoa**
Critério de necessidade – grande interesse para a descoberta da verdade ou para a prova	=	**Critério de necessidade** – grande interesse para a descoberta da verdade ou para a prova

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Procedimentos de selecção e apreensão (inquérito)

"*O **juiz** (que tiver autorizado ou ordenado a diligência) é **a primeira pessoa a tomar conhecimento do conteúdo***"
(artigo 179/3 CPP)

OPC's e Ministério Público tomam primeiro conhecimento

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Procedimentos de selecção e apreensão (inquérito)

"*O **juiz** (que tiver autorizado ou ordenado a diligência) é **a primeira pessoa a tomar conhecimento do conteúdo***"
(artigo 179/3 CPP)

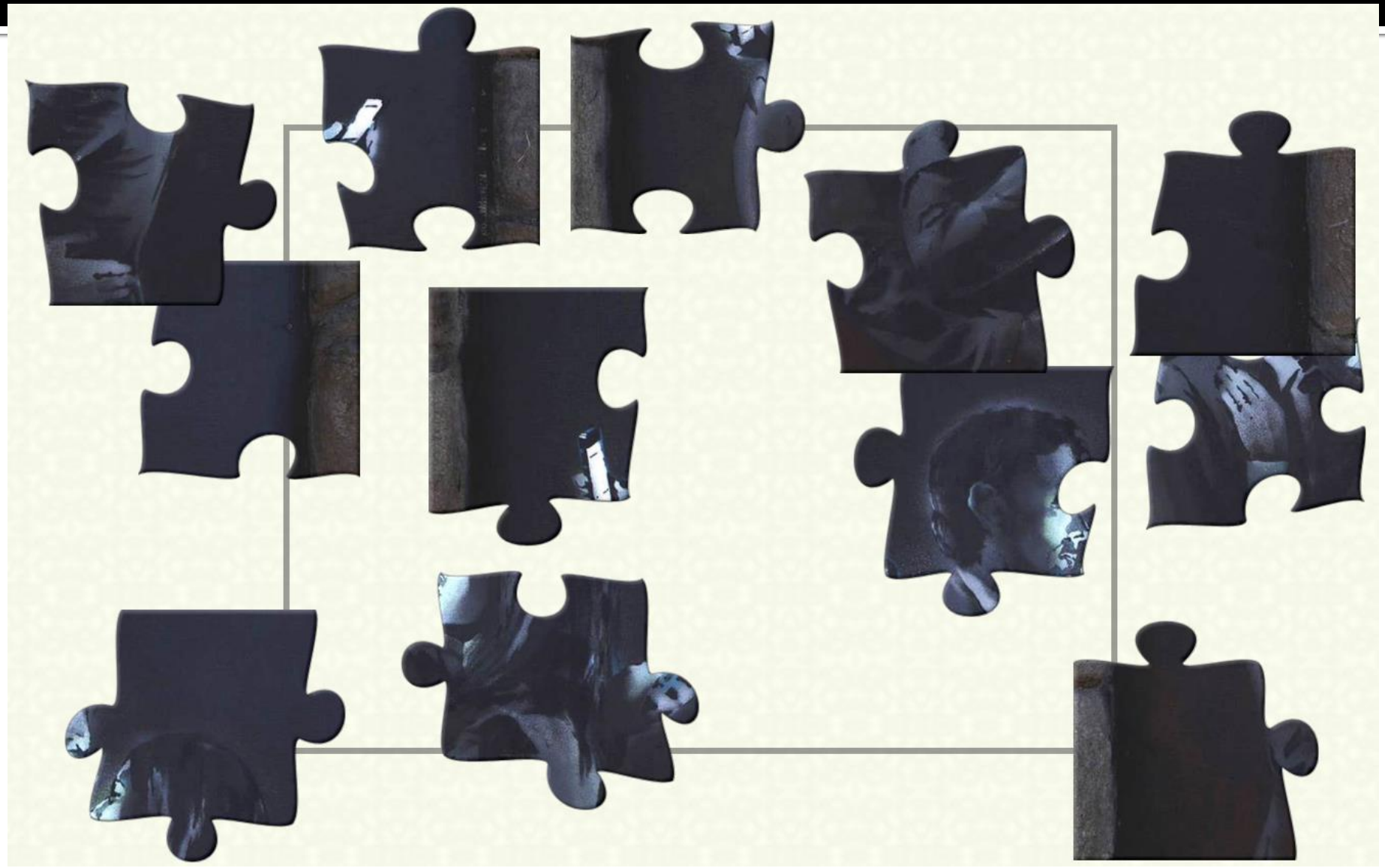
OPC's e Ministério Público tomam primeiro conhecimento

i. Letra da Lei

- Legislador poderia simplesmente ter dito "à apreensão de mensagens de correio electrónico ou registos de comunicações de natureza semelhante é aplicável o regime de apreensão de correspondência previsto no CPP". Não o quis fazer…
- *"… o juiz pode autorizar ou ordenar, por despacho…"*
  - Autorizar pressupõe que a iniciativa é de outrem, do Ministério Público, e que é desse a selecção das comunicações cuja apreensão se autorizará ou não. A não ser assim, o juiz de instrução nunca se limitaria a autorizar, antes sempre ordenaria a apreensão, deixando sem sentido aquilo que o legislador expressamente inseriu na redacção do artigo 17.º.
  - Ministério Público não pode requerer a apreensão das mensagens de correio electrónico ou semelhantes que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova se não as conhece

A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Procedimentos de selecção e apreensão (inquérito)



A CORRESPONDENTE APLICAÇÃO DO REGIME DE APREENSÃO DE CORRESPONDÊNCIA PREVISTO NO CPP

Procedimentos de selecção e apreensão (inquérito)

ii. Coerência do sistema de tutela de direitos

- Nos casos **mais graves** para a privacidade e para o inviolabilidade das telecomunicações dos artigos 16.º, n.º 3, e 18.º, respectivamente, os OPC's e o Ministério Público **podem e devem tomar primeiro conhecimento do conteúdo**; nos casos **menos graves**, quando pode nem sequer existir qualquer violação de privacidade, por que razão é que é **o juiz de instrução** que o deve fazer?
  - *Também nos casos do 16/3 deveria ser o juiz de instrução?*
    - Só com o conhecimento dos mesmos é possível determinar se são ou não susceptíveis de revelar dados pessoais ou íntimos..
    - Legislador recusou essa solução
  - *Mas na intercepção já houve prévia intervenção do juiz de instrução?...*
    - O problema não está no acesso, mas no conhecimento dos dados por parte dos "*não juiz de instrução*": e esse é o mesmo, quer os dados estejam em transmissão, quer estejam já armazenados. A ofensa à privacidade do titular é a mesma.

iii. Diferenças de natureza entre o correio corpóreo e correio electrónico ou semelhante

- **Fundamento para, na apreensão de correspondência, ser o juiz o 1.º a tomar conhecimento** → assegurar que o conteúdo da correspondência estava efectivamente nela contida (não é para impedir que outros que não o juiz tomem conhecimento do conteúdo dessa correspondência em caso de irrelevância probatória)
  - Tal não faz sentido na correspondência electrónica e semelhante: esta **não está fechada, nem é alterável**
- **Não há nenhuma real garantia (*v.g.*, para a privacidade) no conhecimento das mensagens de correio electrónico ou semelhantes ser em primeiro lugar do juiz**: tal não pode impedir o MP de, depois, a essas mensagens ter acesso, nomeadamente para poder recorrer da decisão de não apreensão do juiz.
- **A garantia está apenas na decisão de apreensão/não apreensão** e essa não é minimamente afectada pelo conhecimento prévio pelo MP do conteúdo das mensagens.

iii. Diferenças de natureza entre o correio corpóreo e correio electrónico ou semelhante

- Fundamento para, na [illegible] assegurar que o co[illegible] impedir que outros [illegible] caso de irrelevância [illegible]
  - Tal não faz sen[illegible] ter[illegible]
- [illegible] uma r[illegible] correio electrónico [illegible] depois, a essas me[illegible] apreensão do juiz.
- A garantia está ap[illegible] afectada pelo conheci[illegible]

A (frequente) **operação de "desencapsulamento"** não é minimamente equiparável à abertura de correspondência corpórea prevista no artigo 179.º do CPP.

Dados informáticos "encapsulados" que se supõe serem mensagens de correio electrónico ou semelhantes não são o equivalente a correspondência fechada:

- porque aquela nunca esteve fechada;
- porque não visa (nem consegue) assegurar a integridade do invólucro;
- porque por si não significa tomar conhecimento do conteúdo das mensagens.

iii. Diferenças de natureza entre o correio corpóreo e correio electrónico ou semelhante

- Fundamento para, na
- assegurar que o co
- impedir que outros
- caso de irrelevância
  - Tal não faz sen
  - ter
- N
- correio electrónico
- depois, a essas me
- apreensão do juiz.
- A garantia está ap
- afectada pelo conheci

Incompreensível será também defender que é o juiz de instrução quem primeiro deve tomar conhecimento das mensagens...

... e depois defender que, se o juiz não tiver disponibilidade ou condições técnicas de o fazer, pode devolver os suportes ao Ministério Público sem tomar conhecimento em primeira mão dessas mensagens!

Isso é transformar aquilo que defendem ser uma imposição legal destinada a assegurar direitos fundamentais dos visados num mero poder discricionário do juiz, que o usa apenas quando lhe é possível. A existência da nulidade ficaria assim na dependência da vontade do juiz de instrução, cada um livre de criar o seu regime particular para este meio de obtenção de prova...

iv. Acusatório e competências do juiz de instrução

- **É imperativo constitucional respeitar a função do Ministério Público como titular do inquérito e do juiz de instrução como juiz de garantias**.
- A interpretação conjugada do artigo 17.º da LCC e do artigo 179.º do CPP no sentido de aí fundar uma norma com o sentido de que é o juiz de instrução que, no inquérito, em primeiro lugar toma conhecimento das mensagens de correio electrónico ou semelhantes e que é ele que, oficiosamente, procede à selecção daquelas que são de grande interesse para a descoberta da verdade ou para a prova, para além de **não se traduzir em qualquer real garantia, viola a estrutura acusatória do processo**, pois essa é matéria essencial à direcção do inquérito e à definição do seu objecto, assim comprometendo a posição de imparcial juiz das liberdades.
- A interpretação que criticamos **coloca no juiz de instrução a competência para verdadeiramente investigar os factos noticiados e impor ao Ministério Público a utilização de concretos meios de prova**
- Deve proceder-se a uma **interpretação conforme à Constituição**

PESQUISA – APREENSÃO – JUNÇÃO

1. OPC's procedem à pesquisa / selecção
2. Apresentação ao Ministério Público
3. Ministério Público toma conhecimento e apresenta ao juiz de instrução com requerimento fundamentado, indicando aqueles que são de grande interesse para a prova
   - Em suporte autónomo só com esses dados
   - Dados não estão formalmente apreendidos, mas estão… (por apreensão do suporte ou por cópia)
4. Juiz de instrução aprecia o requerimento do Ministério Público e profere decisão (fundamentada), determinando a apreensão e junção aos autos daqueles que forem de grande interesse para a prova;
   - Os que forem apreendidos, são juntos ao processo (são valoráveis)
   - Se não forem todos os apresentados, terá de se fazer novo suporte só com os apreendidos

Prazos

1. OPC's procedem à pesquisa / selecção
2. Apresentação ao Ministério Público ? 72 h
3. Ministério Público toma conhecimento e apresenta ao juiz de instrução com requerimento fundamentado, indicando aqueles que são de grande interesse para a prova
   - Em suporte autónomo só com esses dados ? 10 d
   - Dados não estão formalmente apreendidos, mas estão… (por apreensão do suporte ou por cópia)
4. Juiz de instrução aprecia o requerimento do Ministério Público e profere decisão (fundamentada), determinando a apreensão e junção aos autos daqueles que forem de grande interesse para a prova;
   - Os que forem apreendidos, são juntos ao processo (são valoráveis) ? 10 d
   - Se não forem todos os apresentados, terá de se fazer novo suporte só com os apreendidos

- **Destino das mensagens de correio electrónico ou semelhantes não apreendidas ?**
  - Destruição?
  - Conservação?
    - Os dados informátic… interceptados, em tempo real, atra… P (*SMS*, *EMS* e *MMS*) ou no artigo 1…
    - Assim, quanto ao re… artigo 179.º do CPP resposta satisfa… da LCC. Sendo os dados da mesma…

Tudo o que não se enquadre no 188/6 CPP deverá manter-se armazenado (188/12 CPP)

Fazendo as necessárias adaptações: o juiz, sem prejuízo do regime dos conhecimentos fortuitos, deve determinar a destruição imediata das mensagens de correio electrónico ou semelhantes que, sendo manifestamente estranhos ao processo, (i) abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado ou (ii) cuja divulgação possa afectar gravemente direitos, liberdades e garantias.

As demais mensagens permanecerão materialmente apreendidas (apreensão cautelar ou provisória). Não poderão, pois, ser destruídas.

- **Destino das mensagens de correio electrónico ou semelhantes não apreendidas ?**
  - Destruição?
  - Conservação?
    - Os dados informátic… interceptados, em tempo real, atra… (*SMS*, *EMS* e *MMS*) ou no artigo 1…
    - Assim, quanto ao re… artigo 179.º do CPP resposta satisfa… da LCC. Sendo os dados da mesma…

TEDH Ac. 04.06.2019 (Sigurður Einarsson e Outros c. Islândia - Queixa n.º 39757/15) – Os requerentes queixaram-se de que a defesa não tinha tido acesso ao vasto volume de dados recolhidos pela acusação durante a fase de inquérito e que não tinha tido uma palavra a dizer na triagem eletrónica desses dados; sustentavam que ninguém tinha revisto a seleção de documentos apresentados ao tribunal e que lhes tinha sido negada a possibilidade de efetuar uma pesquisa utilizando o sistema eletrónico aplicado, o "*Clearwell*", um sistema de *eDiscovery*). O tribunal considerou que seria adequado que tivesse sido dada à defesa a possibilidade de realizar uma busca por provas potencialmente ilibatórias e que **qualquer recusa em autorizar a defesa a fazer novas buscas nos documentos "marcados" levantaria um problema à luz do artigo 6.º §3 (b), relativamente à disponibilização dos meios adequados para a preparação da defesa**

- A LCC não tem previsão expressa sobre esta matéria (só há para escutas – artigo 187/7 e 8)
- A ausência de expressa previsão legal não significa que essa transmissão apenas seja admissível no caso das escutas telefónicas (e, por força do disposto no artigo 18/4 da LCC, também para a intercepção de comunicações):
  - Sendo a prova originalmente válida, a admissibilidade da transmissão verificar-se-á, sem qualquer limitação, sempre que não exista qualquer restrição de âmbito objectivo (catálogo de crimes) ou subjectivo quanto ao concreto meio de obtenção de prova, por razões de economia processual e em obediência a um primado de justiça e procura da verdade material
- No âmbito da LCC:
  - Quaisquer tipos de dados (incluindo os do regime geral, os "sensíveis" e os de correio electrónico e semelhantes)
  - Catálogo do artigo 11/1 LCC (em abstracto, qualquer tipo de crime)
  - Não há qualquer restrição de âmbito subjectivo

1. Pesquisa informática ou outro acesso legítimo a um sistema informático no processo original
2. No processo original, as mensagens poderão estar já apreendidas (artigo 17.º) ou apenas armazenadas (apreensão cautelar)
3. Deverão ser feitas cópias exactas (*hashing*) a remeter ao processo de destino, juntamente com certidão das partes do processo relevantes (despachos, autos de pesquisa e/ou apreensão, validações, etc.)
4. Nenhuma intervenção haverá do juiz de instrução do processo original (se em inquérito)
5. A decisão de apreensão (aferição do "grande interesse para a descoberta da verdade ou para a prova") será do juiz de instrução do processo de destino (o do processo original não o pode fazer)
   - Se apreensão for recusada, os suportes deverão ser devolvidos ao processo original (após trânsito do despacho)

Artigo 18.º

Intercepção de comunicações

1 - **É admissível o recurso à intercepção de comunicações em processos relativos a crimes**:

a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando **tais crimes** se encontrem previstos no artigo 187.º do Código de Processo Penal.

2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o **inquérito**, se houver razões para crer que a diligência é **indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter**, por **despacho fundamentado do juiz de instrução** e **mediante requerimento do Ministério Público**.

3 - A intercepção pode destinar-se ao registo de **dados relativos ao conteúdo** das comunicações ou visar apenas a **recolha e registo de dados de tráfego**, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos **é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal**.

Produção de Prova Digital

E. Intercepção e registo de transmissões de dados informáticos

- **Crimes:**
  - Informáticos (previstos na Lei n.º 109/2009); ou
  - Crimes previstos no artigo 187.º, n.º 1, do CPP, quando cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.
- **Requisitos, pressupostos e trâmites iguais a CPP:**
  - Só no inquérito
  - A requerimento do Ministério Público
  - Por despacho fundamentado por juiz
  - "Indispensabilidade" (se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter)
    - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do CPP (visados, conhecimentos fortuitos / conhecimentos de investigação, prazos, controlos)

Artigo 19.º

Acções encobertas

1 - É admissível o **recurso às acções encobertas previstas na Lei n.º 101/2001,** de 25 de Agosto, nos termos aí previstos, no **decurso de inquérito** relativo aos seguintes crimes:

a) Os **previstos na presente lei**;

b) Os **cometidos por meio de um sistema informático,** quando lhes corresponda, em abstracto, **pena de prisão de máximo superior a 5 anos** ou, ainda que a pena seja inferior, e sendo dolosos, os **crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes**, a **burla qualificada**, a **burla informática e nas comunicações**, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, a **discriminação racial, religiosa ou sexual**, as **infracções económico-financeiras,** bem como os **crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos**.

2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

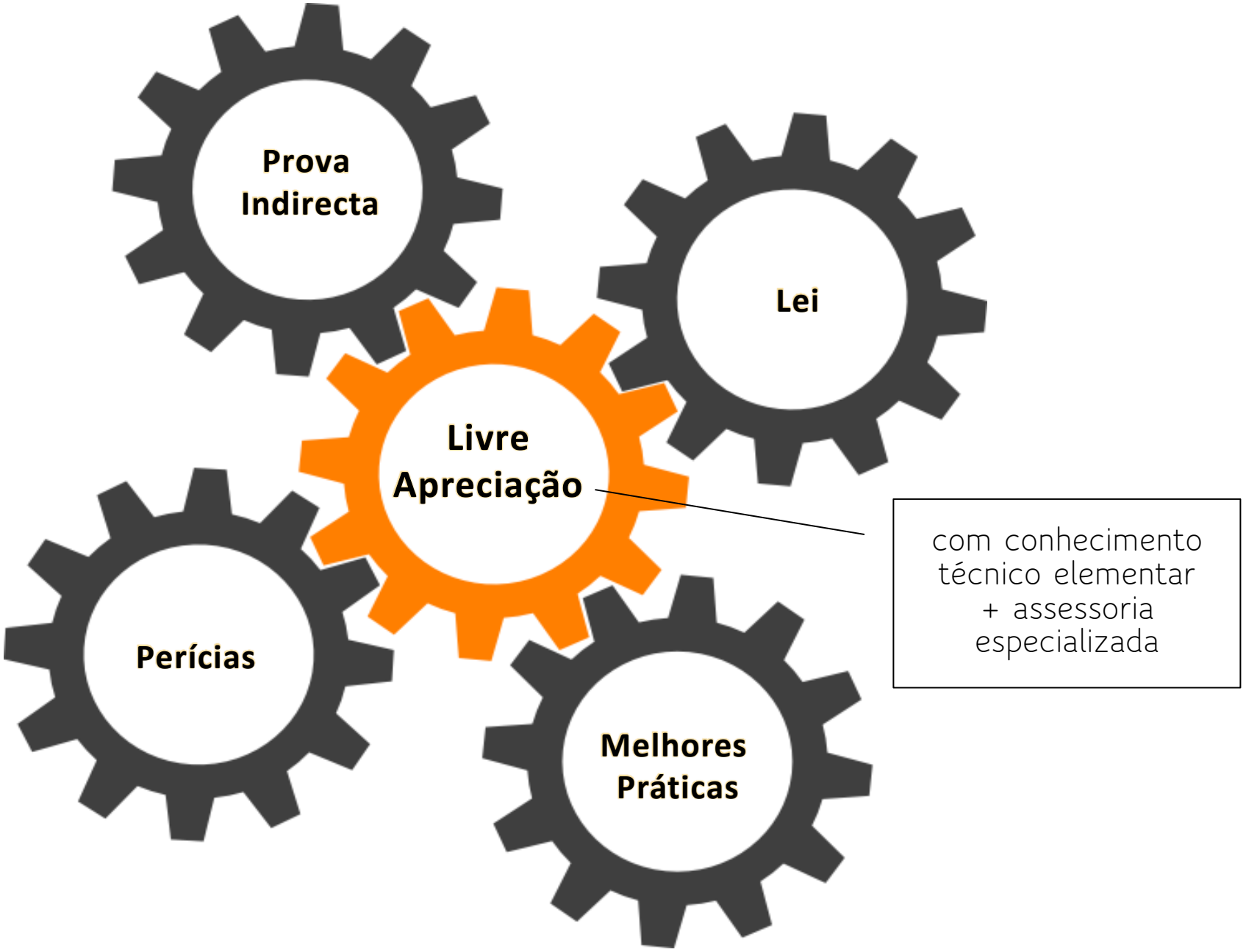
- **Regime das acções encobertas – Lei n.º 101/2001**
  - **Acções encobertas** – aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por **terceiro actuando sob o controlo** da Polícia Judiciária para **prevenção** ou **repressão** dos crimes indicados nessa lei, com **ocultação da sua qualidade e identidade**;
  - **Âmbito de aplicação** – Catálogo de crimes do artigo 2.º
- **LCC - âmbito**
  - Crimes **previstos na LCC**;
  - Crimes **cometidos por meio de um sistema informático**:

dolosos

- quando lhes corresponda, em abstracto, **pena de prisão de máximo superior a 5 anos**
- crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes,
- burla qualificada
- burla informática e nas comunicações
- abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento
- discriminação racial, religiosa ou sexual
- infracções económico-financeiras
- crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos (usurpação, contrafacção, violação do direito moral, aproveitamento de obra contrafeita ou usurpada);

- Acesso ilegítimo?
- Intercepção ilegítima?
- ?

IV. Valoração da prova digital


Prova Indirecta
Lei
Livre Apreciação
Perícias
Melhores Práticas
com conhecimento técnico elementar + assessoria especializada

Prova Digital
no
Crime de Violência Doméstica

Rui Cardoso

Abril | 2022