# Investigação Criminal e Proteção de Dados

Premissas de Discussão

**TIAGO MISAEL DE JESUS MARTINS**

Procurador da República

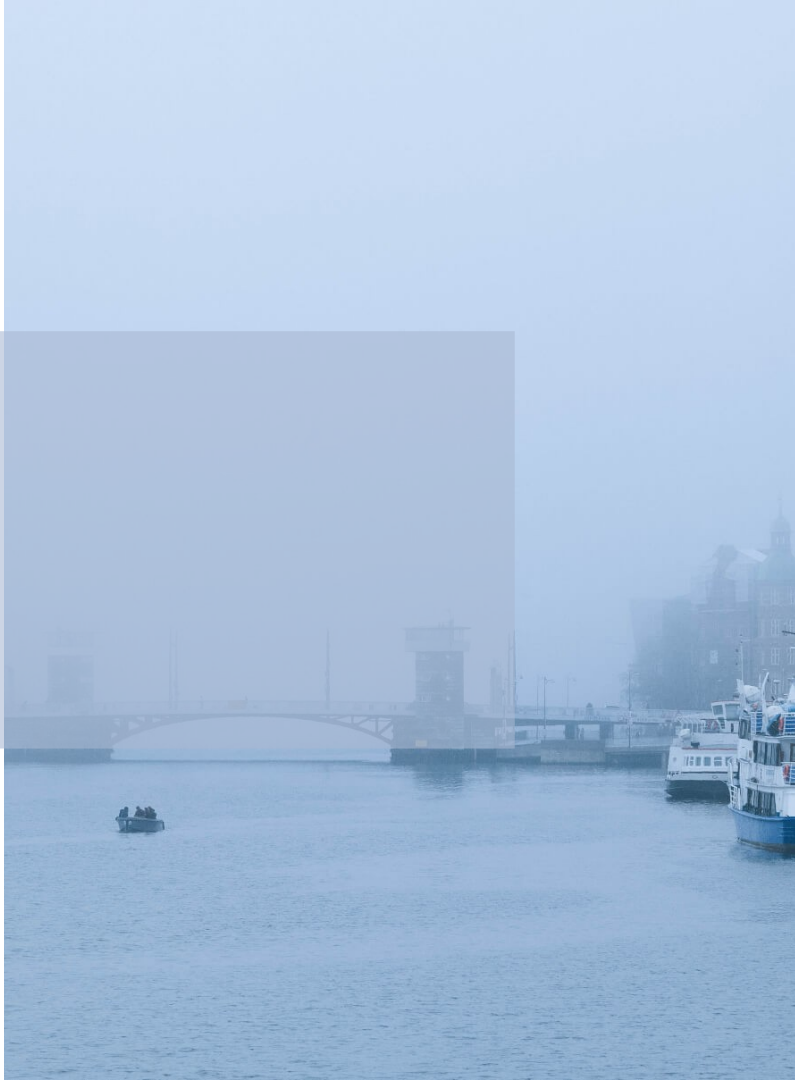
Membro do Grupo de Apoio sobre Criminalidade Cibernética do MPF

Membro do Grupo de Apoio sobre Lavagem de Dinheiro e Investigação Financeira do MPF

Mestre em Direitos Humanos (UFPB)

Autor de *Proibição do Retrocesso Político*

*http://lattes.cnpq.br/1652283673415980*



# Premissa 1

O Estado tem o dever de investigar, processar e punir crimes.

Direito Fundamental à Segurança (art. 5º, caput, CF)

Monopólio da Força
Sistema de Justiça: polícias (art. 144, caput, CF), Ministério Público (art. 127 e ss., CF) e Poder Judiciário (art. 92 e ss., CF).

# Corolário

A investigação, como colheita de elementos de provas, pode implicar o tratamento de **dados pessoais**, **dados pessoais sensíveis** e **dados pessoais sigilosos**, ocasião em que a atividade estatal deve respeitar o **direito fundamental a proteção de dados pessoais** (art. 5º, LXXIX, CF).

# Premissa 2

Em atividade de conformação legislativa, compete ao legislador federal ponderar entre os **direitos fundamentais em colisão** (segurança vs. proteção de dados) e dispor sobre técnicas de investigação (art. 22, I, CF) e tratamento de dados pessoais (art. 22, XXX).

O tratamento de dados pessoais para fins exclusivos de investigação e repressão de infrações penais não estão sujeitos à LGPD (art. 4º, III, d e §1º), mas a legislação específica deverá prever **medidas proporcionais e estritamente necessárias ao atendimento do interesse público**, observados o **devido processo legal**, os **princípios gerais de proteção de dadas** e **os direitos do titular previstos na LGPD**.

**Anteprojeto de LGPD Penal**

# Premissa 3

A lógica das técnicas de investigação dispostas na legislação nacional é a de que elas variam de acordo com a complexidade do crime.

# Técnicas Tradicionais de Investigação

→ apreensão de objetos e instrumentos (art. 6º, II, CPP);

→ oitiva de ofendido, testemunhas e investigado (art. 6º, IV e V, e arts. 185 a 225, CPP);

→ reconhecimento de pessoas ou coisas e acareações (art. 6º, VI, e arts. 226 a 230, CPP);

→ exame de corpo de delito e **qualquer outra perícia** (art. 6º, VI, e arts. 158 a 184, CPP): p. ex., perícia em tecnologia da informação e comunicação;

→ reconstituição de crimes (art. 7º, CPP);

→ **requisição da dados e informações cadastrais (dados de base)** de vítima ou suspeito a qualquer órgãos público ou empresa privada (art. 13-A, CPP; arts. 15 a 17, Lei ORCRIM; e art. 10, §3º, MCI);

→ prova documental (arts. 231 a 238, CPP);

→ **busca e apreensão domiciliar** (arts. 240 a 250, CPP).

# Técnicas Especiais de Investigação

→ colaboração premiada (arts. 4º a 7º, Lei ORCRIM);

→ **captação ambiental** de sinais eletromagnéticos, ópticos ou acústicos (art. 8º-A, Lei 9.269/96);

→ ação controlada (arts. 8º e 9º, Lei ORCRIM);

→ acesso a dados telefônicos (art. 3º, IV, Lei ORCRIM e art. 3º, V, Lei n. 9.472/97);

→ **acesso a dados telemáticos** (art. 7º, III, e art. 10, § 2º, MCI): dados de conteúdo, tráfego e metadados (ex: *geofencing*). Ato preparatório: ordem de preservação (arts. 13, §2º e 15, §2º);

→ interceptação das comunicações telefônicas (art. 1º, Lei 9.269/96);

→ **interceptação das comunicações telemáticas** (art. 1º, parágrafo único, Lei 9.269/96): dados de tráfego e conteúdo. A decisão judicial indicará o meio de execução (art. 4º e 5º);

→ afastamento do sigilo financeiro (LC n. 105/01);

→ afastamento do sigilo fiscal (art. 198, § 1º, I, CTN);

→ **infiltração policial** física e **virtual** (arts. 10 a 14, Lei ORCRIM; e 190-A a 190-E, ECA): limites fixados na decisão judicial;

# Convenção de Budapeste

→ **conservação expedita de dados informáticos armazenados e dados de tráfego** (art. 16 e 17, CB): ordens de preservação de dados (art. 13, § 2º e art. 15, § 2º, MCI);

Obs: **divulgação parcial de dados de tráfego** (art. 17, 1, b).

→ **ordem de injunção** (art. 18, CB): requisição de dados cadastrais (art. 10, §3º, MCI) e quebra telemática (art. 10, § 1º, MCI);

→ **busca e apreensão de dados informáticos armazenados** (art. 19, CB): quebra telemática para a busca remota (art. 7º, III, art. 10, § 2º e art. 22, MCI) e busca e apreensão domiciliar para a busca presencial (arts. 240 a 250, CPP);

→ **recolha em tempo real de dados relativos a tráfego e conteúdo** (arts. 20 e 21, CB)**:** interceptação telemática (art. 1,º, parágrafo único, Lei nº 9.296/96).

Obs: para a **infiltração**, há previsão na Convenção de Palermo (art. 20, 1).

# Premissa 4

As técnicas de investigação, às vezes, são **operacionalizadas** por ferramentas tecnológicas desenvolvidas pelo Estado ou por atores privados.

Ex: SIMBA, SITTEL, SIFISCO, Guardião/Sombra, portais de law enforcement, ferramentas de rastreio de criptoativos, cruzamento de vínculos, *malwares* etc.

# Premissa 5

O tratamento dos dados pessoais, dados pessoais sensíveis e dados pessoais sigilosos, obtidos pelo Estado em investigações criminais, deve obedecer às etapas legais de rastreamento do vestígio para manutenção da **cadeia de custódia** (art. 158-A a 158-F, CPP).

# Premissa 6

A atividade estatal de investigação pode ser **dificultada** por ferramentas tecnológicas.
Ex: criptografia como padrão (*Going Dark Problem*), Rede TOR, criptoativos etc.

# Premissa 7

Ferramentas tecnológicas podem ser empregadas **ilegalmente** por agentes do Estado e atores privados.
Ex: hacking governamental (controle de mensagens, causação de dano e vigilância), ciberespionagem e caso Cambridge Analytica.

*Corolário*: O Estado não pode investigar ilegalmente sob pena de imprestabilidade da prova e responsabilidade do agente.

# Premissa 8

Os dados pessoais coletados pelo Estado legalmente, documentando atividade criminosa específica, representam apenas **pequena parte** dos dados em posse dos destinatários da ordem judicial.

*Corolário*

A ameaça à privacidade das pessoas se apresenta mais séria quando da **coleta massiva de dados** por empresas privadas, no exercício de seus modelos de negócio voltados para publicidade e modelagem de comportamento.

# Conclusão Proposta

É dever do Estado, na realização do direito fundamental da sociedade à segurança, realizar uma investigação cada vez mais tecnológica para processar criminosos e punir crimes cada vez mais tecnológicos, respeitando os direitos fundamentais dos investigados, dentre os quais a proteção de seus dados pessoais.

# Obrigado!

tiagojesus@mpf.mp.br

twitter: **@tiagomjm**