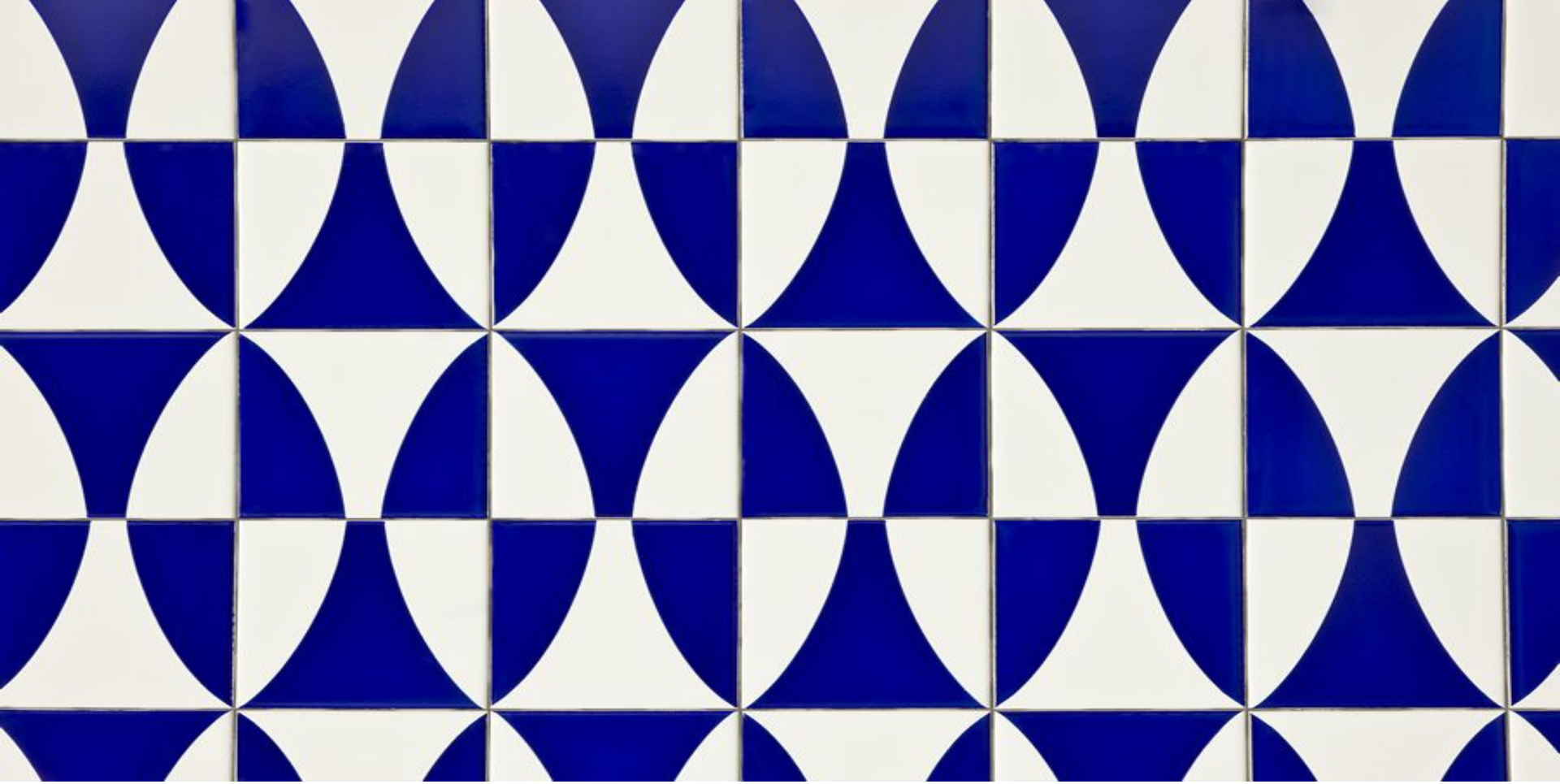


COMISSÃO PARLAMENTAR DE INQUÉRITO - CIBERCRIMES

DENNYS ANTONIALLI
INTERNETLAB

AGENDA

- Garantias e Limites
- Processo de Investigação
- Tipos de Dados
- Princípios Internacionais

AGENDA

- Garantias e Limites
- Processo de Investigação
- Tipos de Dados
- Princípios Internacionais

GARANTIAS E LIMITES

- Liberdade de expressão (CF, art. 5, IX)
- Intimidade e vida privada (CF, art. 5, X)
- Sigilo das comunicações (CF, art. 5, XI)
- Devido processo legal (CF, art. 5, LIV)
- Contraditório e ampla defesa (CF, art. 5, LV)
- Presunção de inocência (CF, art. 5, LVII)

GARANTIAS E LIMITES

- Código de Processo Penal ordena que o juiz observe os princípios da adequação, da necessidade e da proporcionalidade ao ordenar produção de provas (art. 156).
- O mesmo vale para a apreciação de pedidos de medidas cautelares de produção de provas (art. 282).
- Intimação do atingido deve sempre ocorrer "ressalvados casos de urgência e de perigo de ineficácia" (art. 282, § 3o).
- Pela Constituição Federal (art. 5, LVI) e pelo Código de Processo Penal (art. 157), são inadmissíveis provas obtidas por meios ilícitos, contrariando a Constituição ou a lei.

GARANTIAS E LIMITES

- Marco Civil da Internet garante a privacidade e o sigilo das comunicações:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II **- inviolabilidade e sigilo do fluxo de suas comunicações pela internet**, salvo por ordem judicial, na forma da lei;

III - **inviolabilidade e sigilo de suas comunicações privadas armazenadas**, salvo por ordem judicial;

[...]

AGENDA

- Garantias e Limites
- **Processo de Investigação**
- Tipos de Dados
- Princípios Internacionais

PROCESSO DE INVESTIGAÇÃO

PROVEDOR DE APLICAÇÕES (“Registros”)

PROVEDOR DE CONEXÃO

IDENTIFICAÇÃO DO TERMINAL

PROCESSO DE INVESTIGAÇÃO

- Marco Civil da Internet já garante que esses registros sejam retidos:

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos **deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses**, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

PROCESSO DE INVESTIGAÇÃO

- Marco Civil da Internet já garante que esses registros sejam retidos:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o **dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano**, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

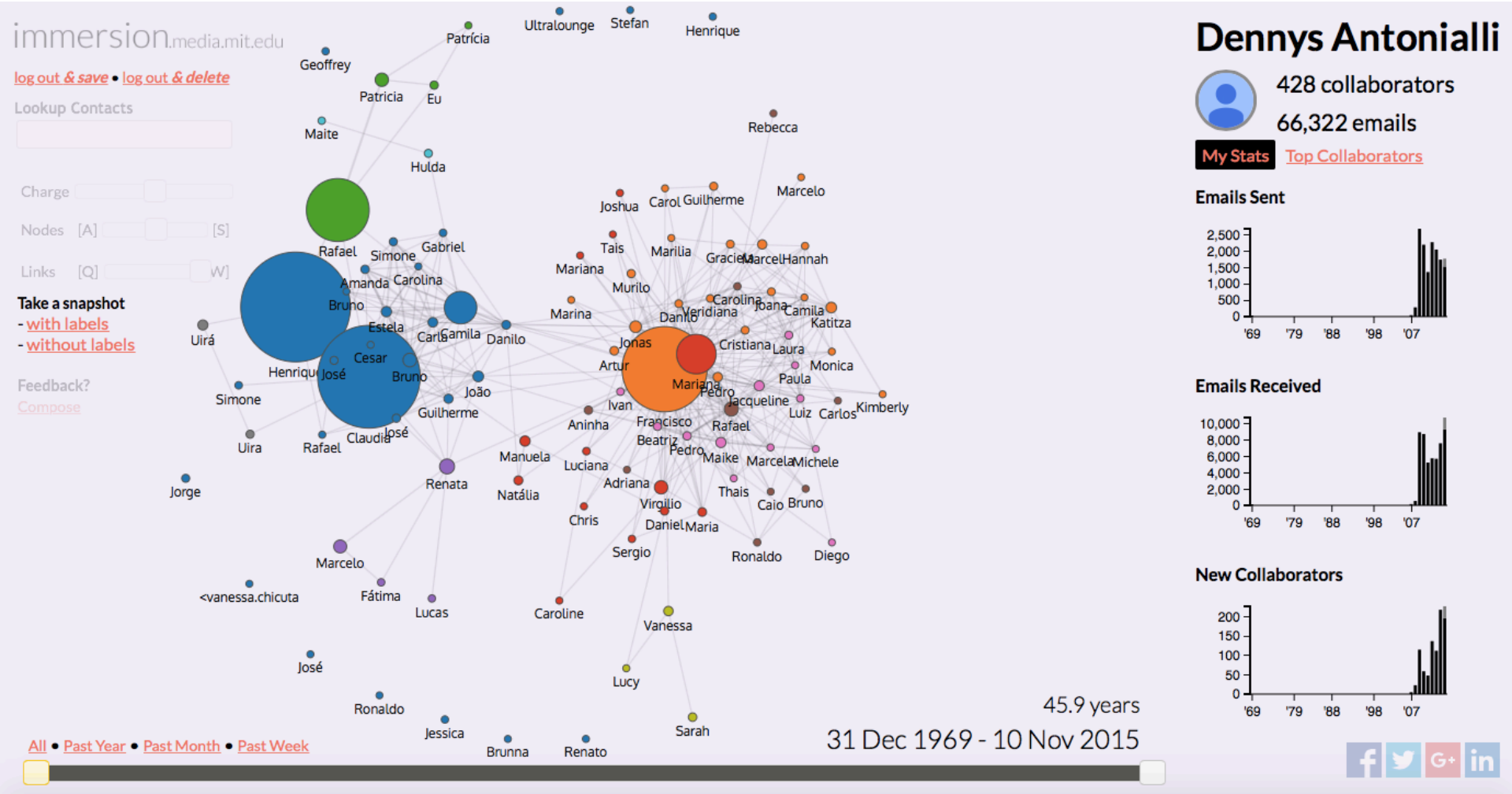
AGENDA

- Garantias e Limites
- Processo de Investigação
- **Tipos de Dados**
- Princípios Internacionais

TIPOS DE DADOS

- Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados
- Registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.
- Metadados: conjunto de dados sobre comunicações com exceção de seu conteúdo
- Não se confundem com conteúdo das comunicações, que pode ser alvo de pedido de remoção

METADADOS


immersion.media.mit.edu
log out & save • log out & delete
Lookup Contacts
Charge
Nodes [A] [S]
Links [Q] W]
Take a snapshot
- with labels
- without labels
Feedback?
Compose
Dennys Antonialli
428 collaborators
66,322 emails
My Stats
Top Collaborators
Emails Sent
2,500
2,000
1,500
1,000
500
0
'69 '79 '88 '98 '07
Emails Received
10,000
8,000
6,000
4,000
2,000
0
'69 '79 '88 '98 '07
New Collaborators
200
150
100
50
0
'69 '79 '88 '98 '07
45.9 years
31 Dec 1969 - 10 Nov 2015
All • Past Year • Past Month • Past Week

AGENDA

- Garantias e Limites
- Processo de Investigação
- Tipos de Dados
- **Princípios Internacionais**

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- LEGALIDADE: Os limites do direito à privacidade devem ser definidos clara e precisamente em leis, e devem ser regularmente revistos pra garantir que as proteções à privacidade prossigam lado à lado com as rápidas mudanças tecnológicas.
- FIM LEGÍTIMO: A vigilância das comunicações so□ deve ser permitida em busca dos objetivos mais importantes do estado.

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- NECESSIDADE: O Estado tem a obrigação de provar que suas atividades de vigilância das comunicações são necessárias pra alcançar um objetivo legítimo.
- ADEQUAÇÃO: Um mecanismo de vigilância das comunicções deve alcançar seu objetivo legítimo efetivamente.
- PROPORCIONALIDADE: A vigilância de comunicações deve ser considerada como um ato altamente intrusivo que interfere com os direitos à privacidade e com a liberdade de expressão e opinião, ameaçando os fundamentos de uma sociedade democrática. A vigilância proporcional vai tipicamente requerer uma autorização prévia de uma autoridade judicial competente.

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- AUTORIDADE JUDICIAL COMPETENTE: Determinações relativas à vigilância de comunicações devem ser expedidas por uma autoridade judicial competente que seja imparcial e independente.
- DEVIDO PROCESSO LEGAL: O devido processo legal requer que qualquer interferência com os direitos humanos seja governada por procedimentos legais, publicamente disponíveis e aplicados consistentemente em uma audiência pública e justa.

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- AUTORIDADE JUDICIAL COMPETENTE: Determinações relativas à vigilância de comunicações devem ser expedidas por uma autoridade judicial competente que seja imparcial e independente.
- DEVIDO PROCESSO LEGAL: O devido processo legal requer que qualquer interferência com os direitos humanos seja governada por procedimentos legais, publicamente disponíveis e aplicados consistentemente em uma audiência pública e justa.

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- NOTIFICAÇÃO DO USUÁRIO: Os indivíduos devem ser notificados de uma decisão autorizando a vigilância de suas comunicações. Exceto quando uma autoridade judicial competente conclua que um aviso prejudicaria a investigação, os indivíduos devem ter uma oportunidade de questionar tal vigilância antes que ela ocorra.
- TRANSPARÊNCIA: O governo tem a obrigçaão de tornar públicas informações suficientes pra que o público em geral possa entender o escopo e a natureza de suas atividades de vigilância. O governo não deve impedir, de um modo geral, que os provedores de serviço publiquem detalhes sobre o escopo e a natureza de seus próprios acordos de vigilância feitos com o Estado.

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- ESCRUTÍNIO PÚBLICO: Estados devem estabelecer mecanismos de fiscalização para garantir a transparência e responsabilização da vigilância de comunicações. Os mecanismos de fiscalização devem ter a autoridade pra acessar todas as informações relevantes a respeito das ações do Estado.
- INTEGRIDADE DAS COMUNICAÇÕES E SISTEMAS: Os provedores de serviço e produtores de hardware ou software não podem ser compelidos a embutir capacidades de vigilância ou monitoramento em seus sistemas, coletar ou reter informação particular apenas para propósitos de vigilância estatais.

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

- SALVAGUARDAS PARA A COOPERAÇÃO INTERNACIONAL: Ocasionalmente, os Estados podem precisar da assistência de provedores de serviço estrangeiros pra conduzir vigilância. Isso deve ser governado por tratados claros e públicos, que garantem que os standards de maior proteção à privacidade devem ser aplicados.
- SALVAGUARDAS CONTRA O ACESSO ILEGÍTIMO: Deve haver penalidades, nas esferas civil e criminal, impostas a qualquer parte responsável pela vigilância ilegal e aqueles afetados por mecanismos de vigilância devem ter acesso a remédios jurídicos efetivos. Também deve ser garantida a proteção daqueles que denunciam atividades de vigilância que afetam direitos humanos

OBRIGADO!

Dennys Antonialli

dennys@internetlab.org.br

www.internetlab.org.br