

# Como identificar agentes maliciosos sem ferir a proteção de dados?

João Brant, Instituto Cultura e Democracia

# Roteiro

- ▶ Temos um problema?
- ▶ Cenário atual
- ▶ Quais as possíveis soluções?

# Temos um problema?

- ▶ A maior parte dos brasileiros se informa via mídia online e redes sociais (esta última ultrapassou a TV em 2020)
- ▶ Entre mais de 40 países pesquisados, Brasil é líder em preocupação com informação falsa ou enganosa: 82% dos brasileiros têm essa preocupação contra 37% na Alemanha.
- ▶ Entre os brasileiros, a leitura é que o WhatsApp é a principal fonte de informações falsas ou enganosas (35%), quase o dobro do Facebook (18%) (números similares em países populosos do Sul Global)

(Digital News Report 2021)

## Temos um problema? (2)

- ▶ Covid: 7 das 10 imagens mais compartilhadas em 522 grupos sobre a pandemia eram falsas (Agência Pública/Monitor WhatsApp UFMG)
- ▶ Eleições de 2018: estudos mostraram rápida viralização de conteúdos (SANTOS e FREITAS, 2019) e predominância de conteúdos falsos em grupos monitorados (Tardaguila, Benevenuto e Ortellado, 2018)
- ▶ WhatsApp tomou medidas importantes para aumentar a fricção. Ainda assim, problema permanece, segundo estudo que envolveu Brasil, Índia e Indonésia:
  - ▶ *Our results suggest that the current efforts deployed by WhatsApp can offer delays on the information spread, but are ineffective in blocking the propagation of misinformation campaigns in public groups.* (Melo P. F., Vieira C.C., Garimella K., de Melo P.O.S.V., Benevenuto F.)

# Cenário atual

- ▶ Aplicativos de natureza híbrida: interpessoal/privada + viral/massa
- ▶ PROBLEMA: funcionalidades não são separadas, nem da perspectiva do serviço, nem da perspectiva regulatória.
- ▶ MAS: paradigma regulatório de serviço privado é aplicado para todo o serviço
- ▶ Número de mensagens com alta viralização: baixo relativamente, alto absolutamente
- ▶ RESULTADO: ambiente opaco + majoritariamente anônimo
- ▶ Impede a responsabilização moral e legal
- ▶ Cria um incentivo sistêmico à desinformação.

# Saídas possíveis

- ▶ Chave está na separação entre as funcionalidades de comunicação interpessoal e a comunicação viral ou de massa
- ▶ Sem uma definição dada pela própria empresa ou pelo usuário, essa fronteira precisa ser desenhada em lei
- ▶ Cenários possíveis:
  - ▶ Não fazer nada ou apostar em soluções já existentes
  - ▶ Aprimoramento do Artigo 10
  - ▶ Modificação do Artigo 10

Sem ilusão de qualquer ‘bala de prata’

# Artigo 10 hoje

- ▶ Força tratamento separado das mensagens interpessoais e virais
- ▶ Guarda apenas metadados
- ▶ Acesso apenas por ordem judicial, quando um receptor descriptografa a mensagem, faz uma reclamação e um juiz decide que há indícios de ilegalidade
- ▶ Todas as outras mensagens que não são encaminhadas para vários destinatários são tratadas como comunicação interpessoal e seus metadados são retidos apenas por quinze dias.
- ▶ **PROBLEMAS APONTADOS:**
  - ▶ Retenção excessiva de dados
  - ▶ Possível ineficácia
  - ▶ Possível uso dos dados em desconformidade com a lei

# Aprimoramento do artigo 10

- ▶ Explicitar a destruição das mensagens que não se tornarem virais depois quinze dias
- ▶ Definir que obrigação não se aplica a mensagens que não sejam encaminháveis
- ▶ Limitar o acesso ao objetivo de constituir prova em investigação criminal ou instrução processual penal pelas práticas de crimes que violem os direitos de crianças e adolescentes; contra a saúde pública; de racismo ou discriminação; estelionato; contra os consumidores; contra a honra; ameaça e crimes eleitorais ou com o propósito de formar conjunto probatório em investigação e processo civil pela prática de ilícito eleitoral.



# Modificação do artigo 10

Art. XX - Os serviços de mensageria privada devem guardar pelo prazo de três meses os registros do envio de **mensagens passíveis de encaminhamento** e o quantitativo de usuários alcançados, resguardado o sigilo do conteúdo das mensagens.

§1º São consideradas mensagens passíveis de encaminhamento aquelas que tenham sido **definidas assim pelo usuário remetente**, por meio de **solução técnica oferecida pelos serviços de mensageria privada**.

§2º Os registros de que trata o caput devem conter:

I - o registro de acesso à aplicação do usuário que **fez o primeiro envio da mensagem**

II - o **identificador** da conta ou número de telefone vinculado ao usuário remetente da primeira mensagem, quando cabível

III - o **quantitativo** total de usuários alcançados por tal conteúdo em todos os encaminhamentos sucessivos, sem indicação individual destes usuários.

§3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento de conteúdo mediante ordem judicial, nos termos da Seção IV do Capítulo III da Lei nº 12.965, de 23 de abril de 2014.

# Vantagens da proposta

- ▶ Empodera o usuário
- ▶ O usuário e as empresas definem fronteira entre mensagens interpessoais e potencialmente virais
- ▶ Guarda-se apenas o primeiro remetente, sem risco de afetar mensagens interpessoais
- ▶ Guarda-se o quantitativo de destinatários alcançados, sem precisar definir quais