



Instituto
de Tecnologia
& Sociedade
do Rio

Rastreabilidade e crimes cibernéticos

Fabro Steibel
ofabro@itsrio.org
2/dez/21

Audiência pública

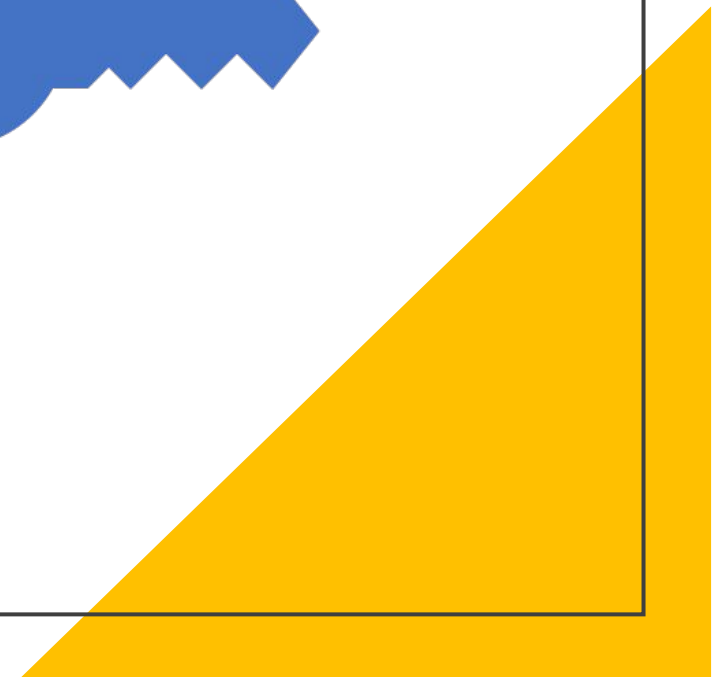
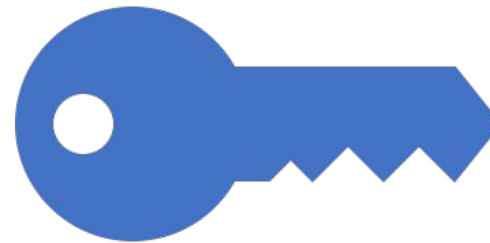


A rastreabilidade vs. Escuta de metadados

A yellow right-angled triangle is positioned in the bottom right corner of the slide, pointing towards the top-left.

Mito 1 – Rastreabilidade não quebra a criptografia

Criptografia é um conjunto de protocolos





Política

Hackers usaram código do Telegram para acessar celular de Moro, diz PF

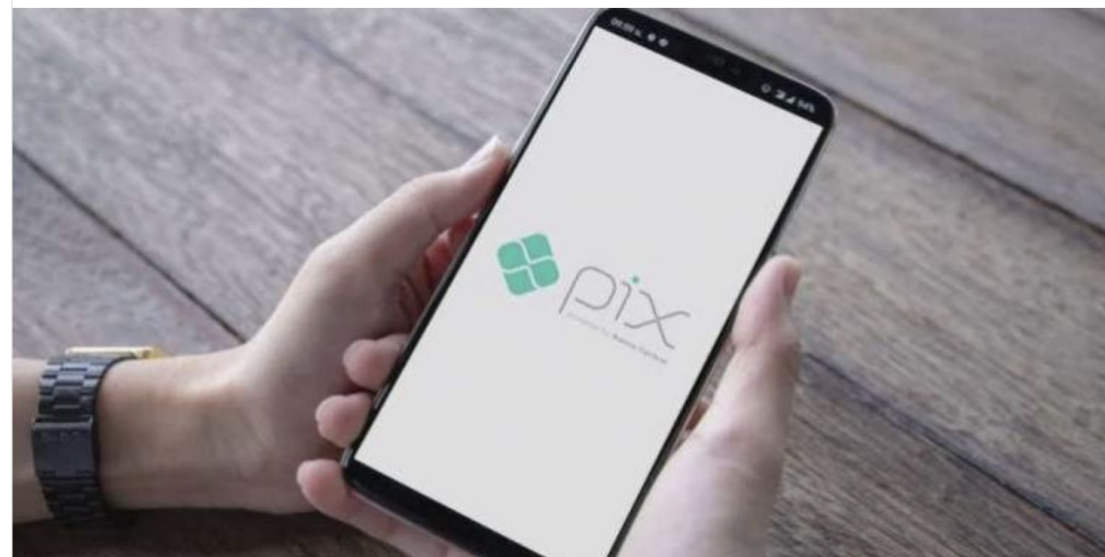
Operação Spoofing, deflagrada pela Polícia Federal, investiga atuação de hackers na invasão de celulares do ministro Sergio Moro

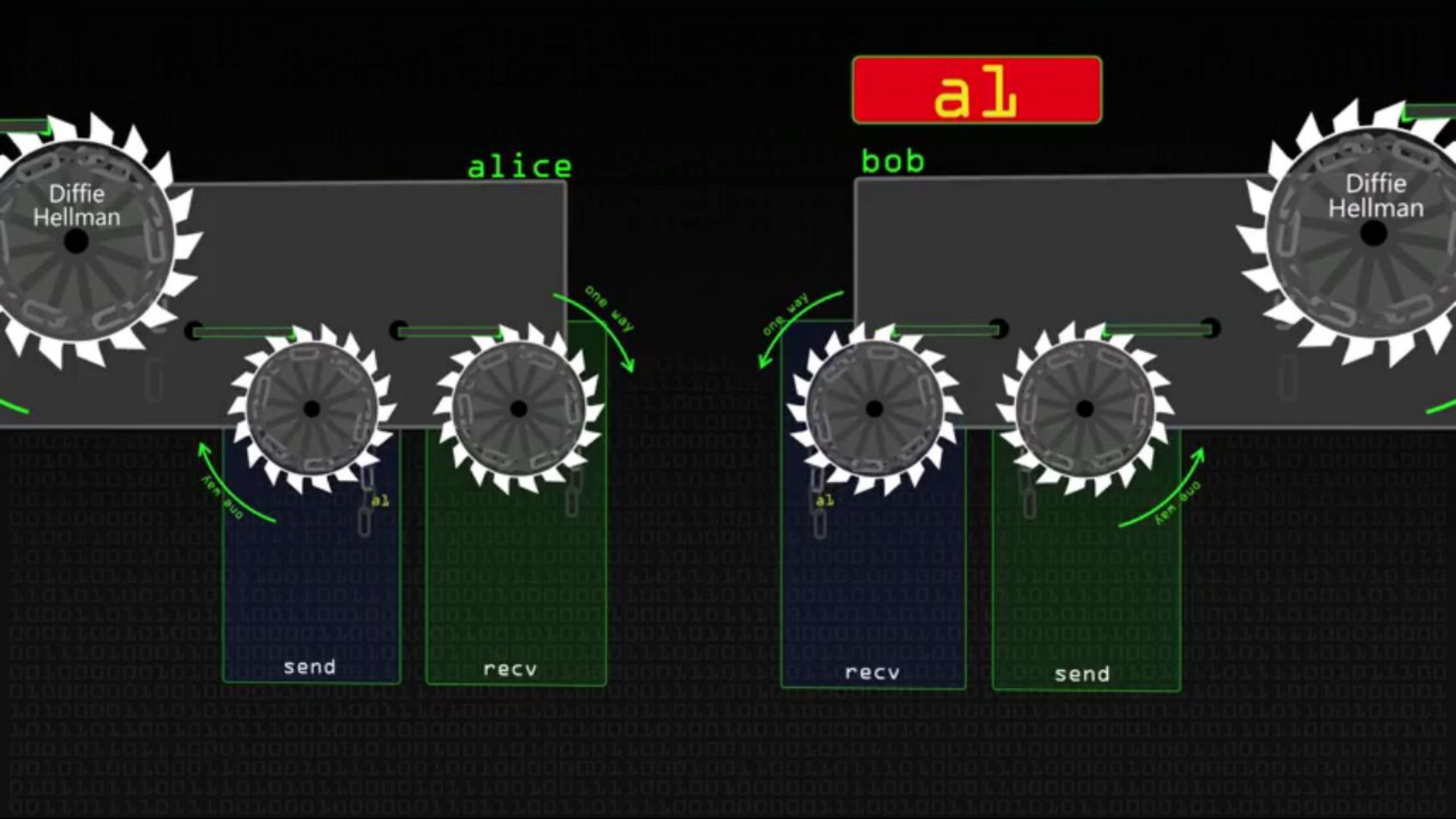
Por **Leonardo Lellis**

© 24 jul 2019, 14h33 - Publicado em 24 jul 2019, 12h36

ECONOMIA

BC comunica vazamento de dados de chaves Pix em instituição financeira





a_1

alice

bob

Diffie Hellman

Diffie Hellman

send

recv

recv

send

one way

one way

key

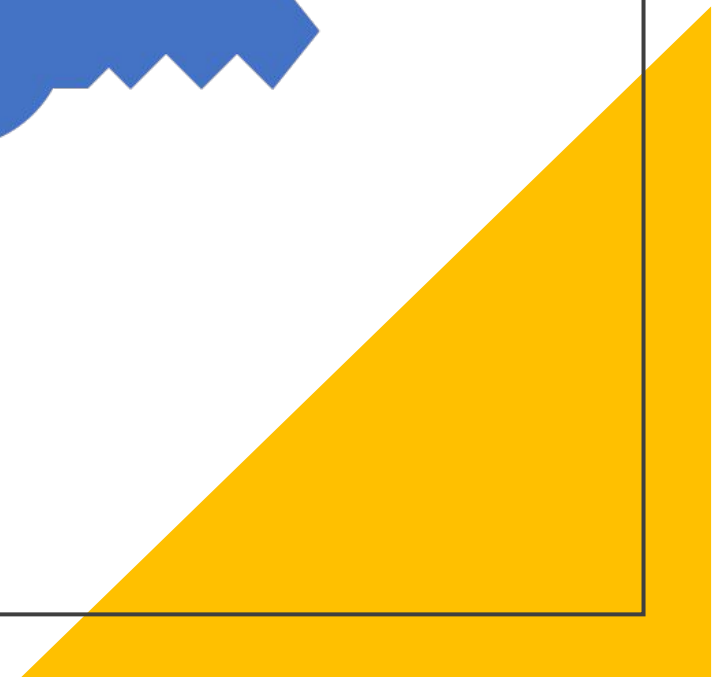
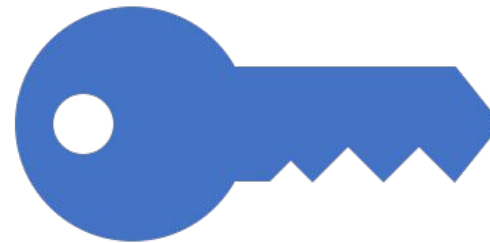
a_1

a_1


key

Mito 2 –
Rastreabilidade não
revela conteúdo


Banco de hashes são galinhas de ouro







User: Fulano
Senha: 12345
Salt: XYZ
Hash(12345+XYZ):
e5c5ec94023c839c53ab88bd7c184100



User: Fulana
Senha: 12345
Salt: ABC
Hash(12345+ABC):
185aef3b1c810799a6be8314abf6512c

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

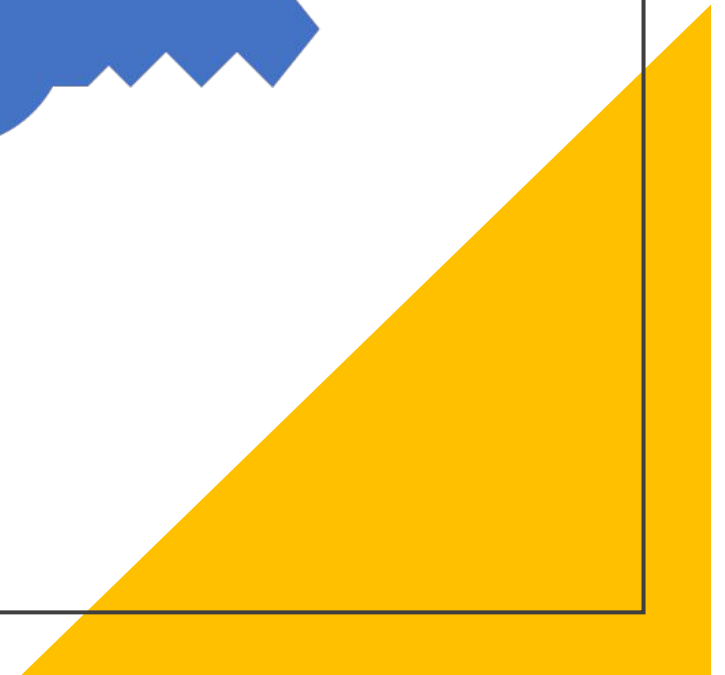
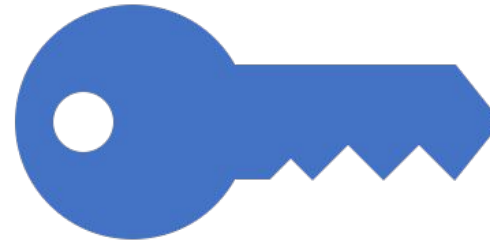
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

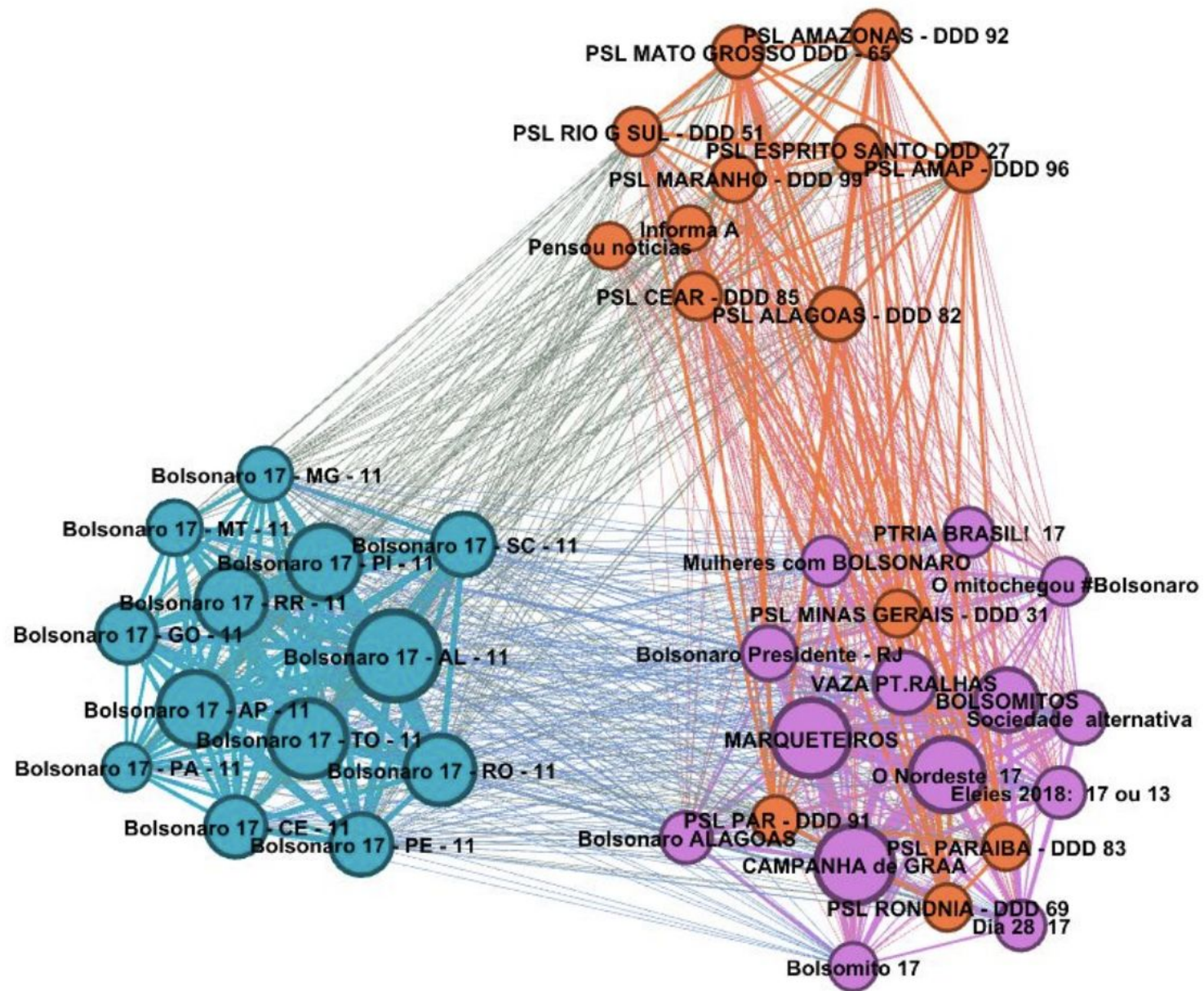


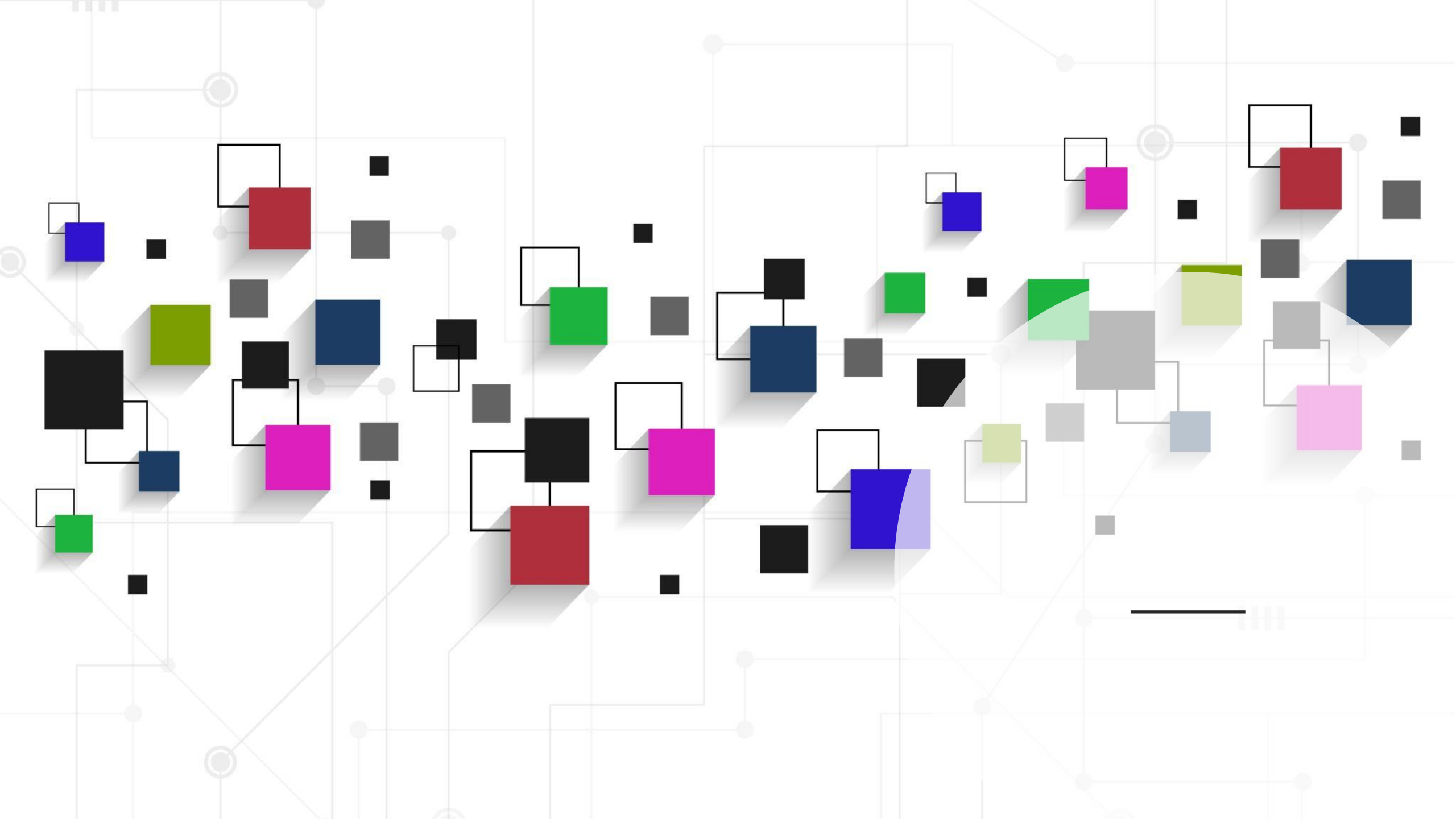
-Data sourced from [HowSecureismyPassword.net](https://howsecureismypassword.net)

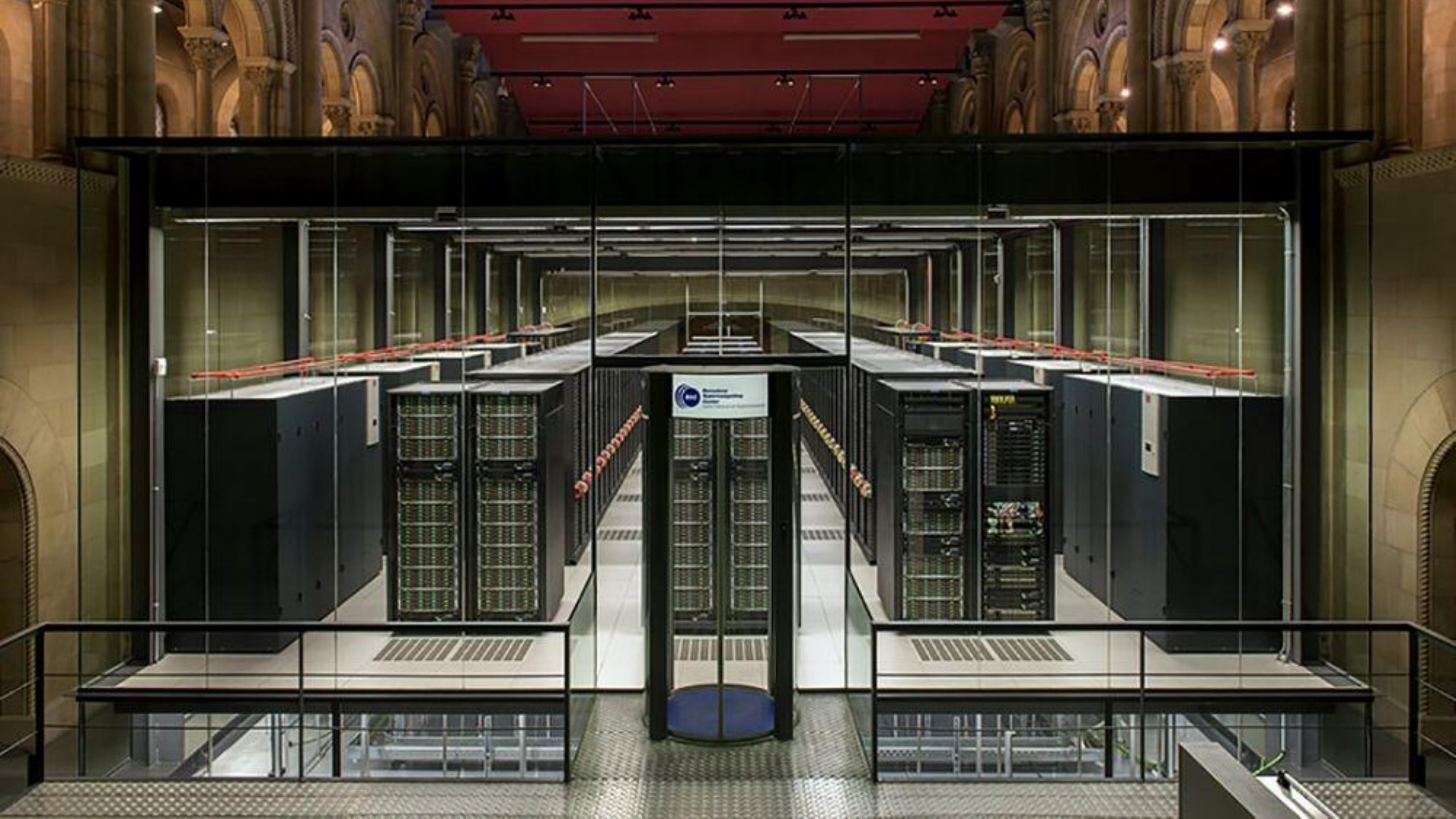
Mito 3 – Rastreabilidade é eficiente para investigação

*Nunca foi testado o poder computacional
necessário para analisar os dados*









A rastreabilidade vs. Escuta de metadados

A yellow right-angled triangle is positioned in the bottom right corner of the slide, pointing towards the top-left.

ROBERT FARIS,
AND HAL ROBERTS

NETWORK PROPAGANDA

<https://soundcloud.com/berkmanklein/network-propaganda-manipulation-disinformation-and-radicalization-in-american-politics>

MANIPULATION,

FBI Document Says the Feds Can Get Your WhatsApp Data — in Real Time

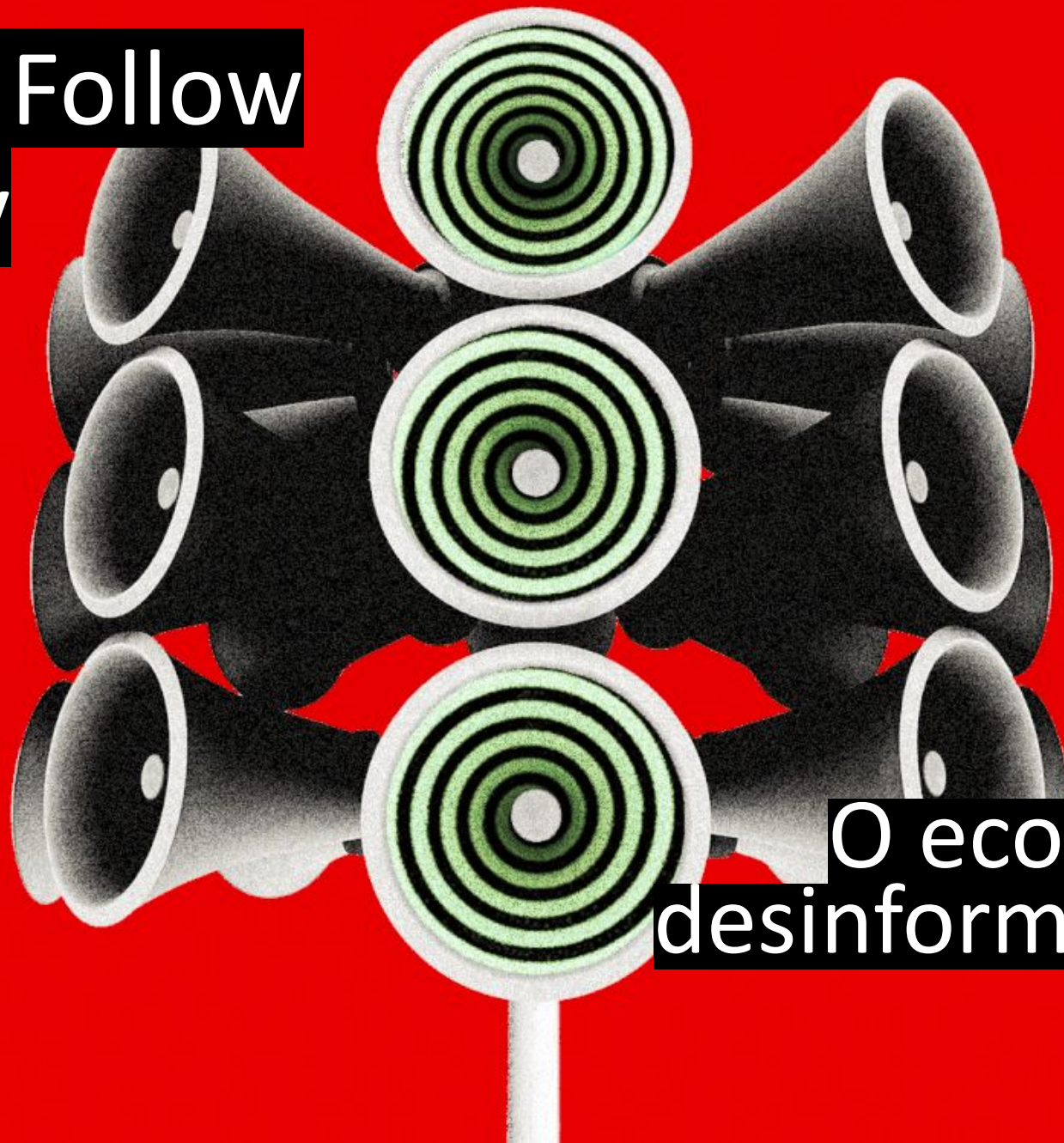
A previously unreported FBI document obtained by *Rolling Stone* reveals that “private” messaging apps WhatsApp and iMessage are deeply vulnerable to law-enforcement searches

By **ANDY KROLL** 



The J. Edgar Hoover FBI building in Washington Nov. 30, 2017 (AP Photo/Carolyn Kaster)

Regulação Follow
the money



O ecossistema da
desinformação É uma
indústria



Instituto
de Tecnologia
& Sociedade
do Rio

Rastreabilidade e crimes cibernéticos

Fabro Steibel
ofabro@itsrio.org
2/dez/21

Audiência pública

