Re-criptografando o presente - Lidando com o Invisível

Devemos confiar no visível?

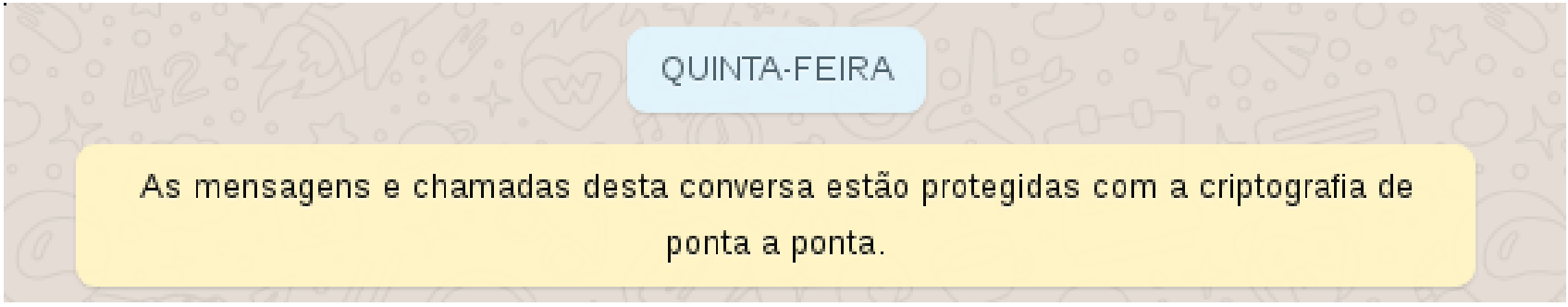
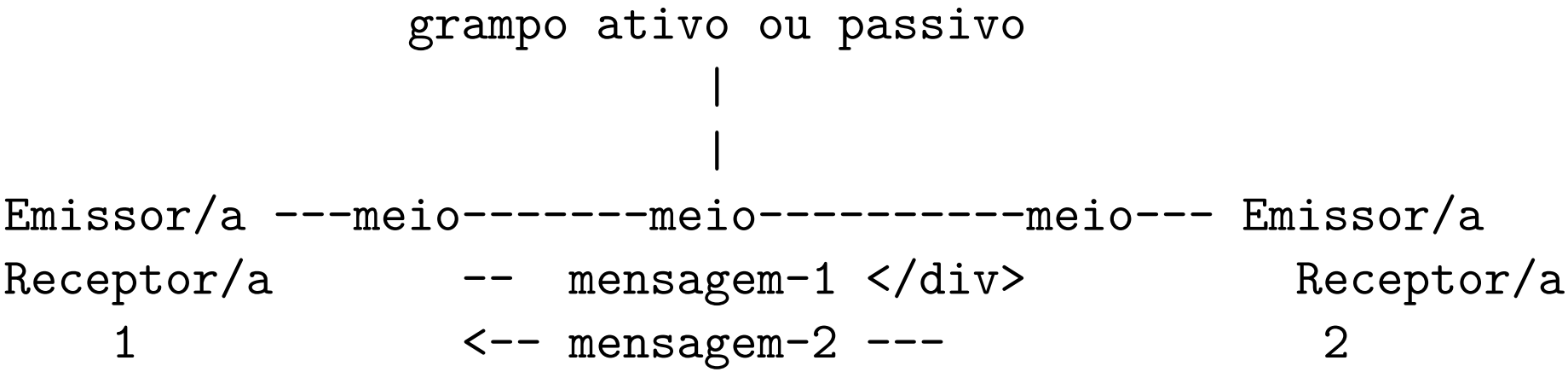


Figura 1: Aviso do WhatsApp sobre “criptografia de ponta-a-ponta”

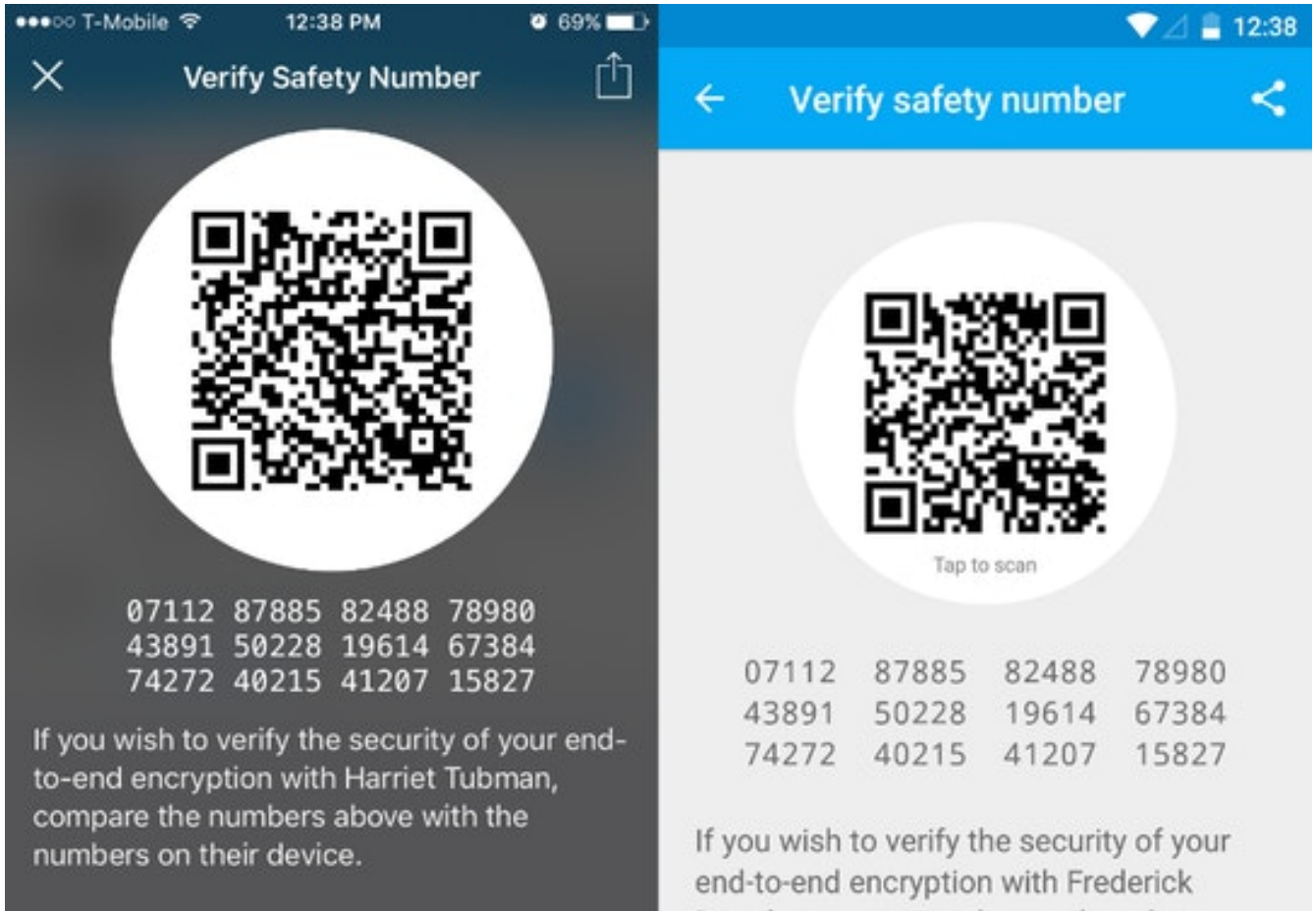
O que esta pequena afirmação significa? Criptografia...



- Regra geral prática: se uma comunicação *pode* ser grampeada, assuma que ela está sendo grampeada. Assim fica mais fácil se prevenir *sempre.*
- Proteja sempre que possível a comunicação com criptografia.

. . . de ponta-a-ponta

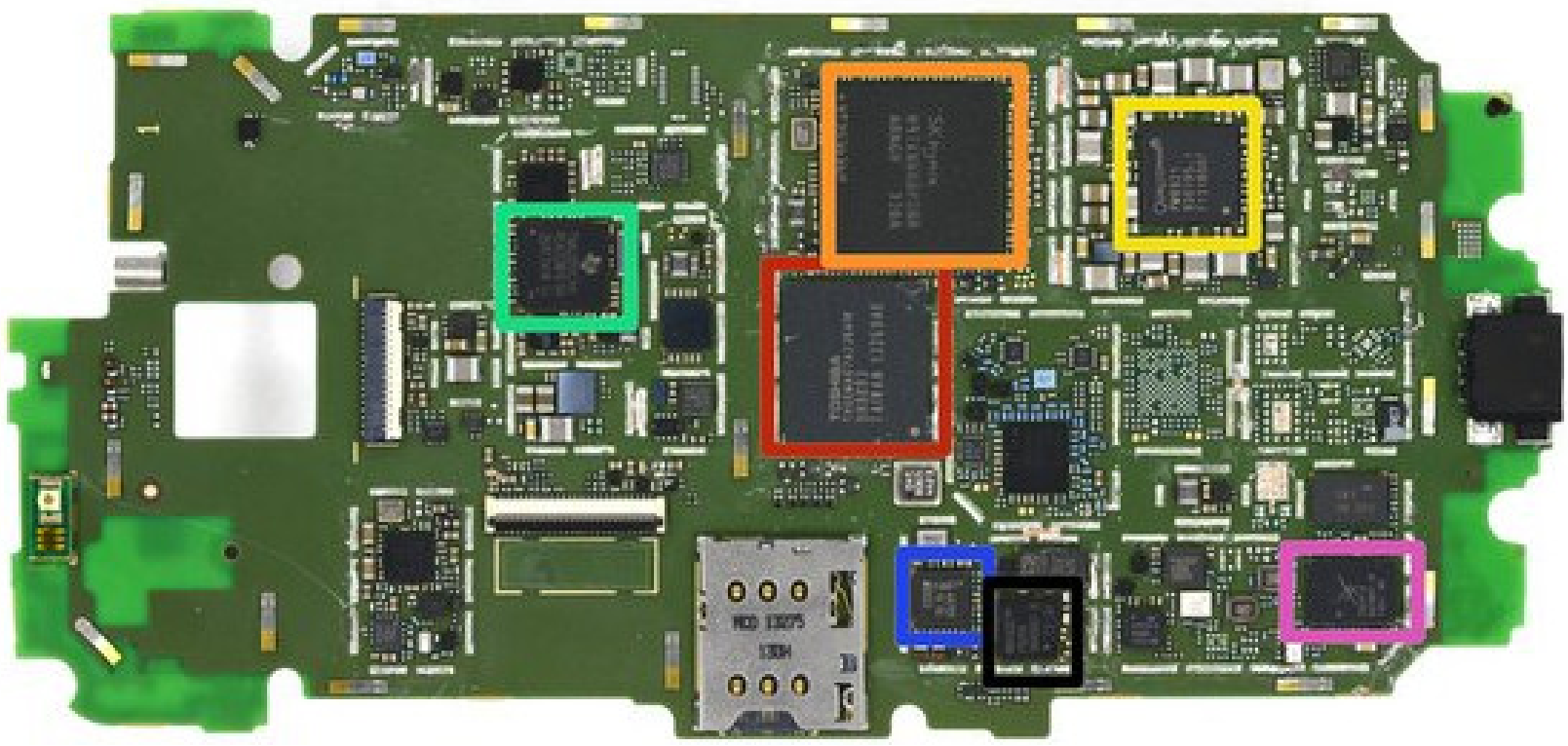
- Use preferencialmente criptografia de ponta-a-ponta.
- Operações de criptografar/descriptografar acontecem no dispositivo da pessoa.
- As pessoas tem como confirmar o **número de segurança** da conversa com outra pessoa.



Em quais lugares esta afirmação está inscrita?

Nas redes digitais, o próprio meio é um conjunto enorme de emissores/receptores, cada qual passível de grampo.

Em qualquer lugar no caminho da comunicação, do dispositivo emissor até o receptor, as mensagens podem ou não estar criptografadas. Podem ou não estar grampeadas.

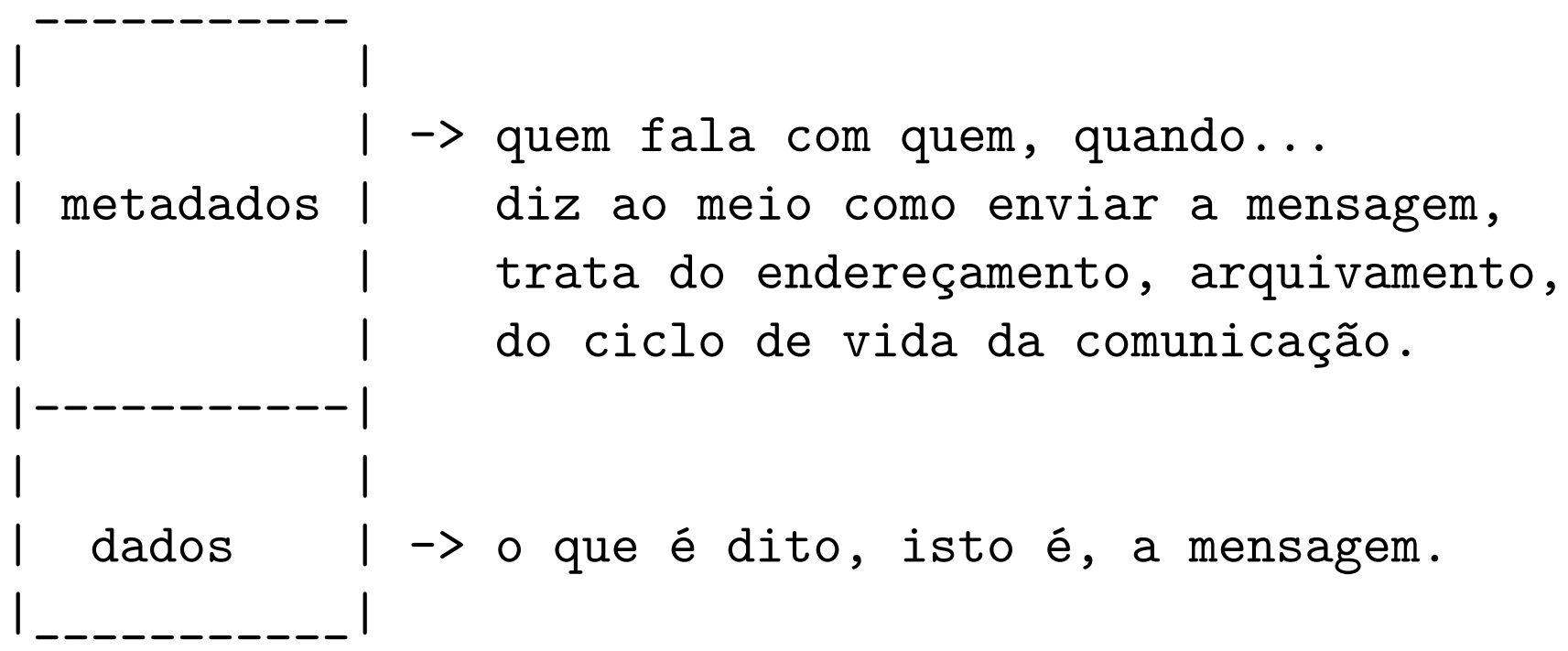


Esta afirmação é mesmo verdade?

- Não temos como dizer quando o **o código do aplicativo estiver fechado.**
- Mesmo que os dados estejam criptografados:
  - Os metadados podem não estar. Provavelmente não estão. E eles dizem muito...
  - Seu dispositivo pode estar comprometido e a comunicação vazar quando estiver decifrada.
  - Autoridades podem ser incluídas na conversa como mais uma das pontas cifradas.

Metadados? Dispositivo comprometido? Autoridades???

Metadados: dados de atividade



Também pode ser informação de uso: quanto tempo a pessoa usou o aplicativo etc.

Dispositivo comprometido

Falhas de segurança:

- Por conta da concepção/design do dispositivo, do sistema e do aplicativo.
- Durante o processo de construção.
- Falta de atualização.
- Problemas de configuração.

Cada dispositivo tem vários pontos onde pode ser atacado. Para quem pode, há muita documentação sobre como protegê-los melhor.

Autoridades

- WhatsApp apresentou a Moro iniciativas para colaborar com a Justiça. Não sabemos quais exatamente. Podemos imaginar...
- PL 9808/2018 - "Acrescenta os parágrafos 5° e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica".

Como assim?

- É possível implementar chave de custódia, sem violar a criptografia de ponta-a-ponta do aplicativo bastando adicionar um "destinatário interno" para qualquer comunicação de interesse.
- É possível, ainda, que a plataforma forneça os metadados às autoridades, via Marco Civil (art. 15 da Lei 12965/2019) e/ou Lei do Grampo (Lei 9296/1998).
- O WhatsApp passa a ser, além de disseminador relâmpago de informações falsas, o paraíso dos espiões computadorizados.

O que seria isso, então?

Figura 4: Oocistos espurulados, com quatro esporozoítos cada!

Cryptosporidium

Cryptosporidium é um gênero de protozoário apicomplexo que pode causar criptosporidíase, um tipo de diarreia que afeta humanos e outros animais. A transmissão dos oocistos é fecal-oral. Pode ser prevenido filtrando ou fervendo a água antes de beber e cozinhando bem os alimentos, não ingerindo-os crus.

-- https://pt.wikipedia.org/wiki/Cryptosporidium

Ilusões de Segurança

- Aplicativos fechados, que se anunciam como criptografados de ponta-a-ponta mas que coletam e processam metadados e que podem fornecer sua comunicação quando pressionados são **Cryptosporidiuns Digitais,** ocasionando a diarréia da sua comunicação!
- A doença pode ser prevenida com software, hardware e serviços livres que tenham criptografia forte, de ponta-a-ponta, bem implementada, auditada e com cadeia de produção mais justa.
- Mas estamos vivendo uma epidemia e as medidas preventivas não são facilmente aplicáveis pra qualquer pessoa. . . :(

Imagens de Insegurança

Figura 5: Que delícia! Mas tá cheia de salmonela!

Como (não) fazer visível o invisível?

Figura 6: Campanha da Gangrena do Ministério da Saúde

Não se pode esconder a cadeia produtiva

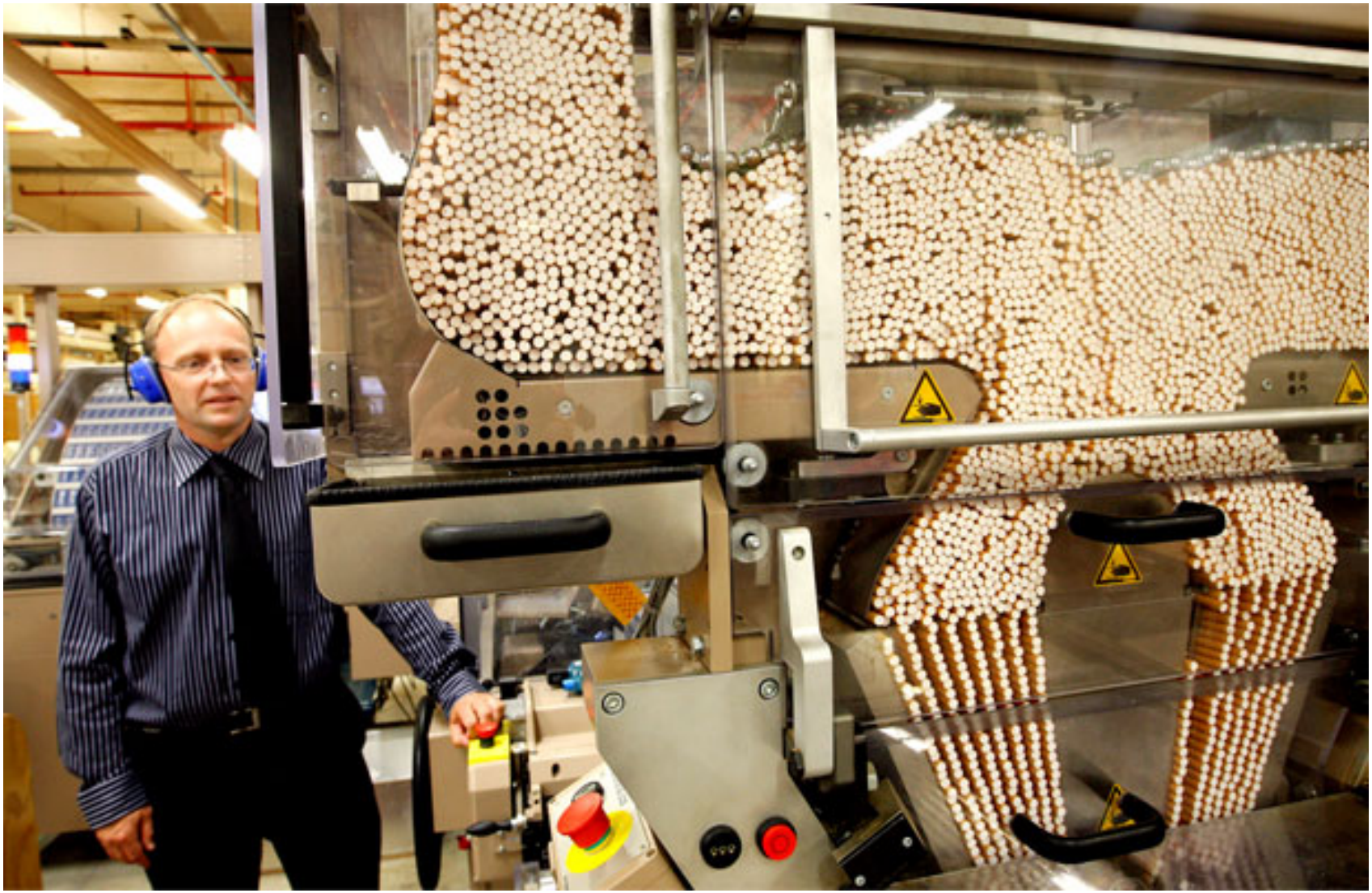


Figura 7: Perigo invisível do fósforo ainda não riscado...

Choque de Realidade

Figura 8: Recordista fuma 153 em 1983 usando um ventilador

Um cigarro nunca é só um cigarro

Figura 9: Campanha Tochas da Liberdade, do sobrinho de Freud, 1929

Tecnologias do Vício são vendidas como Plataformas de Prazer

- A coleta de dados e metadados e a manipulação de usuários(as) consistem nos principais processos do Capitalismo de Vigilância.
- Se focarmos o debate apenas no campo estritamente tecnológico (e isso é possível?) ou político (na visão estrita de "ativistas políticos" demandando privacidade), deixamos de lado os processos mais importantes.
- Há uma campanha em curso para que cada pessoa seja mais um terminal conectado constantemente ao aparato de dominação.

O Texto-Sombra

- Conceito-chave Shoshana Zuboff em seu recente livro "The Age of Surveillance Capitalism" (2019).
- O "texto principal" é aquele que consta na comunicação entre as pessoas e serviços. São as mensagens que trocamos.
- O texto-sombra (shadow text) é aquele que é produzido através da análise dos dados extraídos das pessoas, sejam dados, sejam metadados.
- O texto-sombra é inacessível às pessoas, mas está disponível aos administradores(as) das plataformas. Essa assimetria cria a "divisão do aprendizado" e estabelece uma distinção dura: "Quem sabe? Quem decide? Quem decide quem decide?"
- Zuboff argumenta que apenas adotar criptografia é insuficiente, apenas um remendo para um sistema que está quebrado em seu núcleo, a assimetria de conhecimento gerando desigualdades sociais.

Perguntas em aberto

- Estratégia de Conscientização: como mostrar a realidade nua e crua sem provocar aversão, alienação e escapismo?
- É importante fazer campanhas não só alertando problemas, mas sobretudo disputando a narrativa. Mas quais são as narrativas que podem ser instigantes a ponto de contestar o Admirável Mundo Novo?
- Mostrar alternativas possíveis de viver são suficientes? E se a servidão continuar sendo mais fácil?

Então é isso aí

- Perguntas?
- Contato: rhatto@riseup.net