



CODA·BR



↑ ESCOLA DE DADOS
→ x



Da Biometria aos Data Centers: conflitos entre Progresso e Direito Digital

Thallita Lima (Panóptico/ CESeC)

Valentina Luza (Amaranta)



NESTE WORKSHOP, VAMOS VER...

- Direitos digitais e desenvolvimento científico-tecnológico
- Dados biométricos: entre o acesso e a flexibilização de direitos
- Centralização de dados: grandes Data Centers
- Como (re)imaginar o uso de dados: práticas cidadãs de produção de dados sobre os usos de dados nas políticas públicas

Dados Biométricos: O que São e
Por que Exigem Proteção?

Dado biométrico é uma informação única de características físicas, fisiológicas ou comportamentais usadas para identificação automática.

A Lei Geral de Proteção de Dados (LGPD) estabelece que dados biométricos são tipos de dados pessoais sensíveis. Ou seja, estão relacionados à pessoa identificada ou identificável.

Acesso a Direitos

- Facilitando o acesso a serviços públicos, como saúde e educação.
- Identificação e verificação de identidade para benefícios sociais.
- Inclusão de indivíduos sem documentos tradicionais.

Questões problemáticas

- Privacidade e segurança dos dados biométricos.
- Possibilidade de vazamento e uso indevido de informações.
- Discriminação e uso indevido pelos governos ou empresas.

Centralização de Dados

- Riscos de Segurança e Privacidade

Exemplo: Vazamento de dados no Ministério da Saúde (ConecteSUS) expôs dados sensíveis de milhões de brasileiros, evidenciando fragilidades na proteção.

- Aumento de Disparidades de Poder

Exemplo: O sistema CórTEX no Brasil, que concentra dados de segurança pública, levanta questões sobre vigilância massiva e a falta de transparência no acesso

Exemplo: da Municipalidad de las Condes foi usado no Chile. Foram gastos cerca de 45 milhões na implementação e houve cerca de 2% de assertividade.

- Dependência de Infraestruturas Não Sustentáveis e caras

Os **Data centers** **Data** centers consomem até 1,3% da energia global, aumentando significativamente a pegada de carbono, além dos grandes volumes de água.

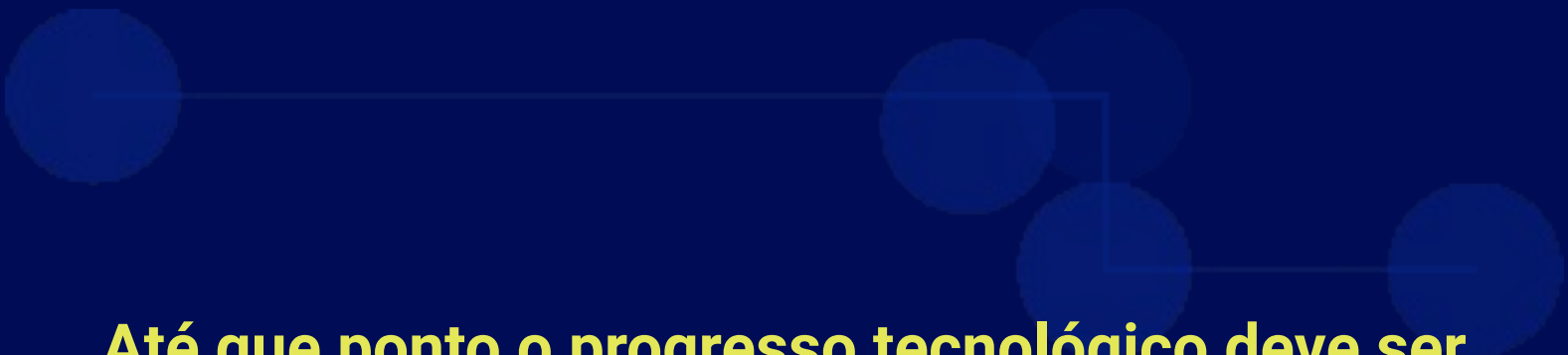
No Chile, há 4

Caminhos possíveis

Descentralização: Utilizar modelos distribuídos e federados para reduzir vulnerabilidades.

Sustentabilidade: Adotar práticas de eficiência energética e uso de energia renovável em data centers.

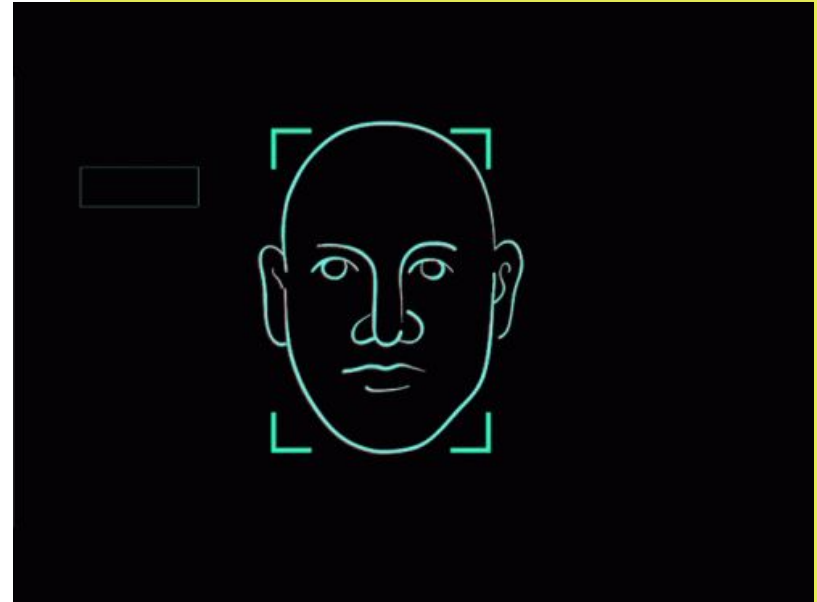
Transparência e Governança Cidadã: Estabelecer marcos regulatórios claros e possibilitar a auditoria dos sistemas.



Até que ponto o progresso tecnológico deve ser priorizado em relação à proteção de direitos individuais?

Direitos Digitais e Desenvolvimento Científico-Tecnológico

- As tecnologias biométricas, e a “solução” para questões de identificação
- Promessas: eficiência, inclusão e segurança
- Desafios no uso de biometria para inclusão social versus potencial discriminação.



Dados Biométricos: Entre o Acesso e a Flexibilização de Direitos

- Impactos no Brasil, com destaque para sistemas como o **Córtex** e outras **plataformas integradas de monitoramento**.
- Casos de abuso ou uso indevido de dados biométricos (ex.: problemas de viés em algoritmos de reconhecimento facial).
- Casos de abuso: No Chile, a empresa WordIcon coletou informações sobre mais de 200.000 mil chilenos sem declarar explicitamente o que significava fornecer essas informações.
-

RECONHECIMENTO FACIAL USADO PELO GOVERNO PODE EXCLUIR TRANS E NEGROS

MARINA OLIVEIRA

27.01.2021 10:08 ● 2

Em [GOVERNO](#)
TEMAS

[CIÊNCIA E TECNOLOGIA](#)
[DIREITOS HUMANOS](#)

TAGS

[INSS NEGROS](#) [ENEM](#) [SERPRO](#) [LGPD](#)
[LEI GERAL DE PROTEÇÃO DE](#)
[DADOS](#)
[TRANS](#) [MEI](#) [TRAVESTIS](#)
[PESSOAS NEGRAS](#)



Documentos obtidos por meio da [Lei de Acesso à Informação](#) mostram que a tecnologia utilizada para reconhecimento facial em aplicativos do governo federal como o “gov.br” pode levar a situações de exclusão e discriminação de cidadãos. Dados revelados pelo [estudo inédito da Coding Rights](#) revelam que a tecnologia empregada em serviços do INSS, por exemplo, valida somente 64,32% das biometrias realizadas.

A ferramenta “gov.br”, que permite a criação de uma conta para solicitar serviços digitais da União, como Meu INSS, CTPS Digital, Enem, eCAC, MEI, entre outras funções, muitas vezes “automatiza e massifica preconceitos e estigmas sociais”, dizem as pesquisadoras Mariah Rafaela Silva e Joana Varon, responsáveis pelo estudo.



APOIE

ÚLTIMAS NOTÍCIAS

18:46

De Trump a Fernanda Torres: veja personalidades que serão premiadas pela Câmara

16:50

Prioridade absoluta, também nas telas

15:56

Haddad e Bolsonaro começam o jogo para 2026

Fonte: <https://congressoemfoco.uol.com.br/temas/direitos-humanos/reconhecimento-facial-pode-excluir-trans-e-negros-de-servicos-publicos/>

200 mil chilenos han "vendido" su iris: ¿Qué es y cuáles son los peligros de "Worldcoin"?

Por **Javiera Rodríguez** | **Daniel Silva**
12 mar. 2024 - 21:40 hrs.

Compartir



¿Qué pasó?

Cada vez se ha hecho más usual ver filas de personas para que una bola de metal les escanee sus ojos. Esto se puede ver tanto en centros comerciales como en la vía pública y ya **casi 200 mil chilenos han "vendido" sus iris** por un poco más de \$20 mil en criptomonedas

200.000 chilenos
“venderam” suas
íris: o que é isso e
quais são os
perigos da
“Worldcoin”?

[200 mil chilenos han "vendido" su iris: ¿Qué es y cuáles son los peligros de "Worldcoin"? - Meganoticias](#)

Ao entregar dados biométricos a uma entidade com operações opacas, **os usuários se expõem a riscos de longo prazo, como roubo de identidade ou uso indevido de suas informações pessoais.**

- **Amaranta ONG**

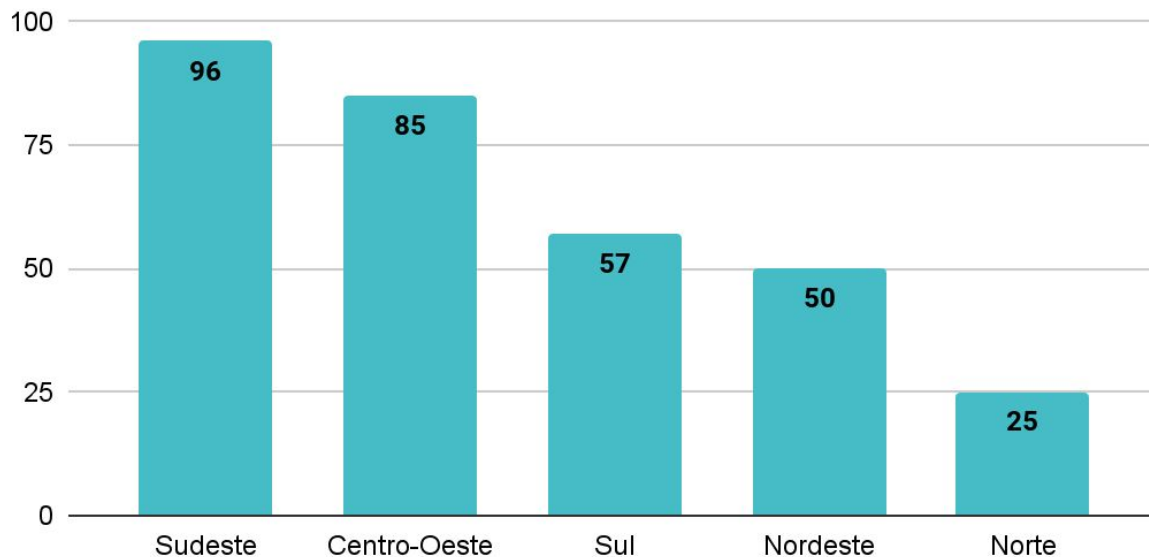
Reconhecimento facial na segurança pública

313 projetos
utilizando
tecnologia de
reconhecimento
facial no Brasil.

79 milhões de
cidadãos estão sob
potencial
vigilância.

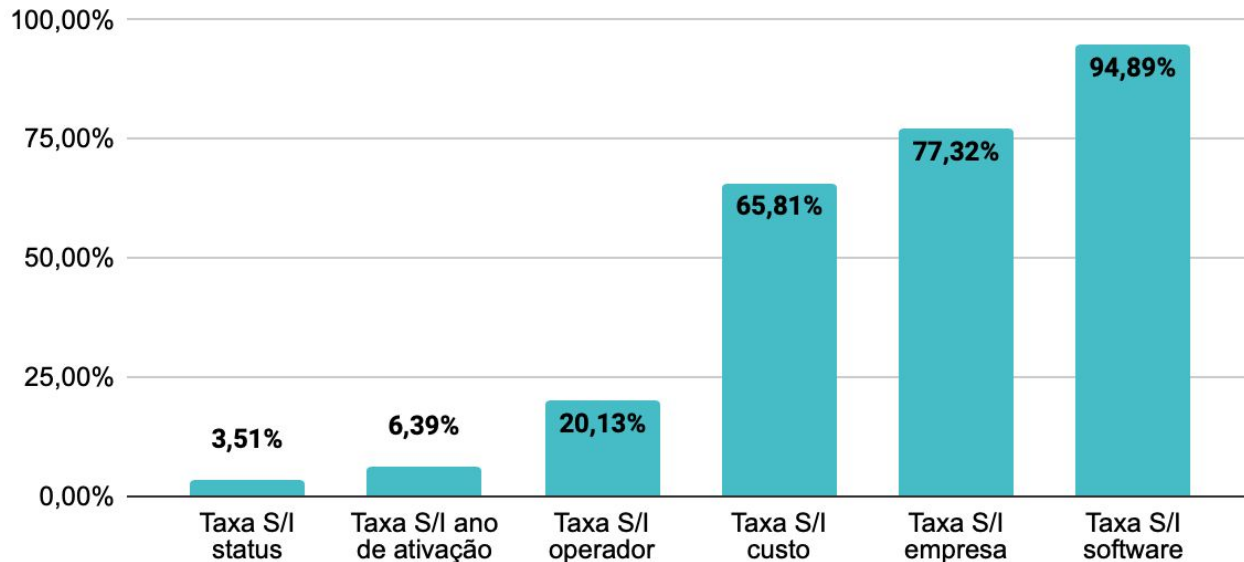


Número de projetos de reconhecimento facial ativos no Brasil por região (2018 a 2024*)




Fonte: O Panóptico | CESeC. *Dado compreende até outubro de 2024


Taxa de sem informação dos projetos ativos de reconhecimento facial no Brasil



Fonte: O Panóptico | CESeC, 2024.



“Muito do que é rotineiro, razoável, intuitivo e codificado reproduz arranjos sociais injustos, sem nunca queimar uma cruz para lançar luz sobre o problema.”



Devemos refletir como a produção de dados e o uso de tecnologias são ideologicamente moldadas pelas noções de gênero e raça vigentes na nossa sociedade.

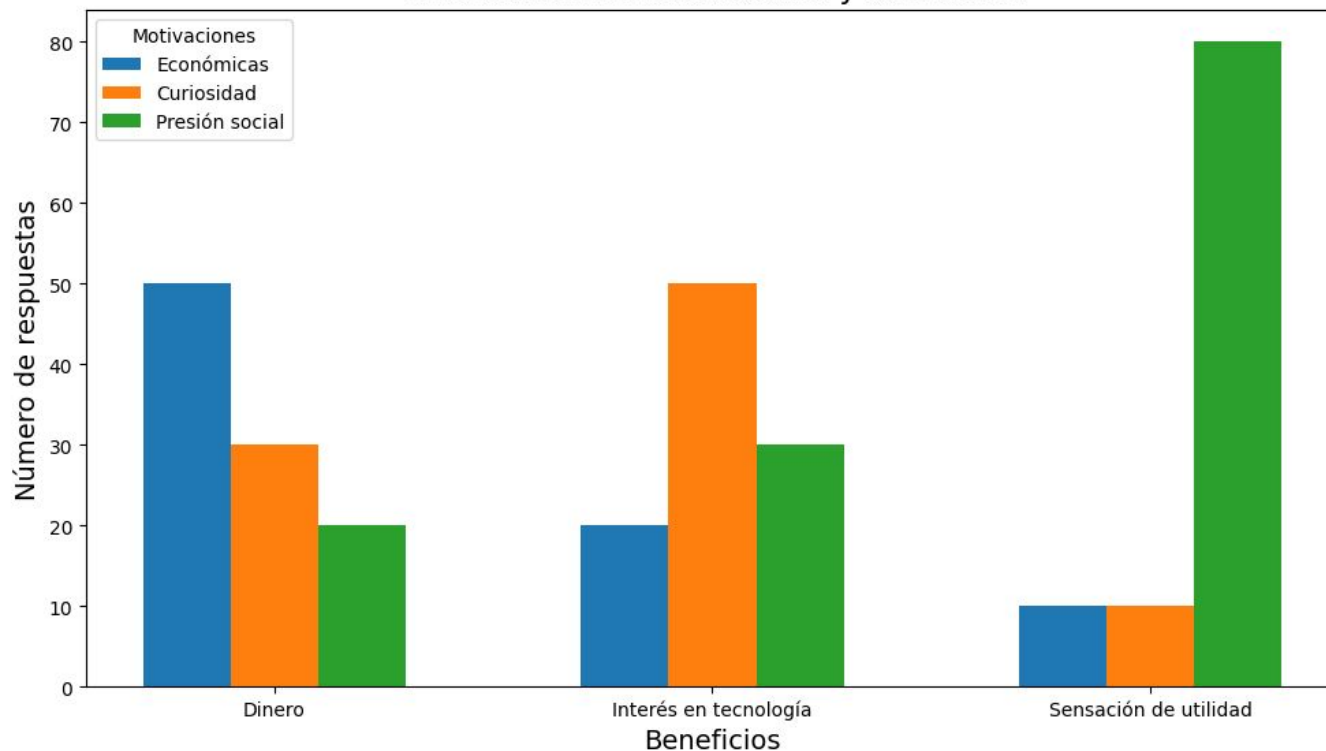
E isso inclui as tecnologias biométricas. Em um mundo onde cada vez mais nossos dados biométricos estão sendo armazenados e usados por empresas e governos, como podemos pensar em caminhos possíveis?

**Venda de dados pessoais sem
consentimento**

Atualmente, há 22 centros de escaneamento em operação e um centro de operações da empresa.

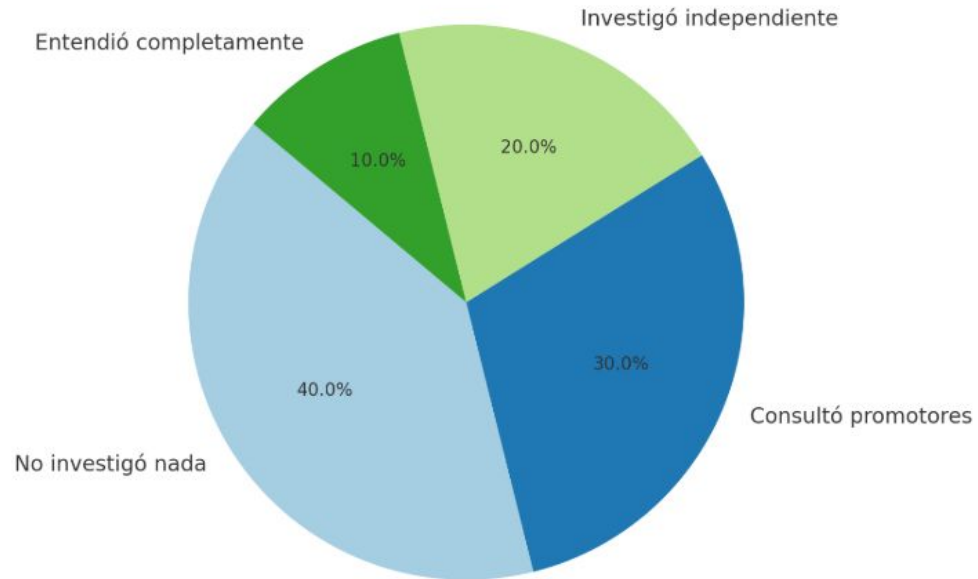


Relación entre Motivaciones y Beneficios




Fonte. Amaranta ONG. Pesquisa: **VENDENDO DADOS BIOMÉTRICOS PARA A WORLDCOIN NO CHILE: AUSÊNCIAS E VULNERABILIDADES LEGAIS EM UM PAÍS EM DÍVIDA COM A PROTEÇÃO DE DADOS (2024)**


Niveles de Conocimiento sobre WorldCoin

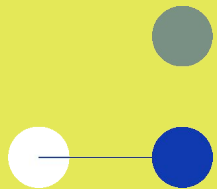


Fonte. Amaranta ONG.Pesquisa: **VENDENDO DADOS BIOMÉTRICOS PARA A WORLD COIN NO CHILE: AUSÊNCIAS E VULNERABILIDADES LEGAIS EM UM PAÍS EM DÍVIDA COM A PROTEÇÃO DE DADOS (2024)**

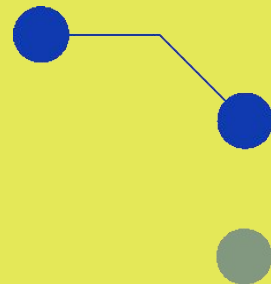


“A coleta de dados biométricos, especialmente sem uma estrutura legal robusta, gera sérias preocupações com a privacidade”. Portanto, ele acrescenta, “é fundamental que os consumidores entendam as possíveis repercussões de longo prazo da entrega desses dados”.





Como (re)imaginar o uso de dados?



Modelos **alternativos** de gestão de dados

- Práticas cidadãs de monitoramento de tecnologias, como o Panóptico
- Coleta descentralizada e ética no uso de dados.
- Exemplos internacionais e boas práticas: dados abertos e uso em políticas públicas.
- Convocação para uma governança inclusiva e transparente.

Modelos **alternativos** de gestão de dados

- Implementar a proteção adequada dos dados mantidos pelo Estado. É importante que essas informações não acabem nas **mãos de terceiros** - como aconteceu com várias violações de segurança do Serviço Eleitoral, gerando os sites de rutificação - e que haja verificação de identidade suficiente em suas plataformas para evitar comportamentos mal-intencionados, como falsificação de **identidade e doxing**.

Muito obrigada!

○ PANÓPTICO

@panopticobr

thallitalima@cesecseguranca.com.br

www.opanoptico.com.br



@amarantaong

violen.amarantas@gmail.com

www.amarantas.org