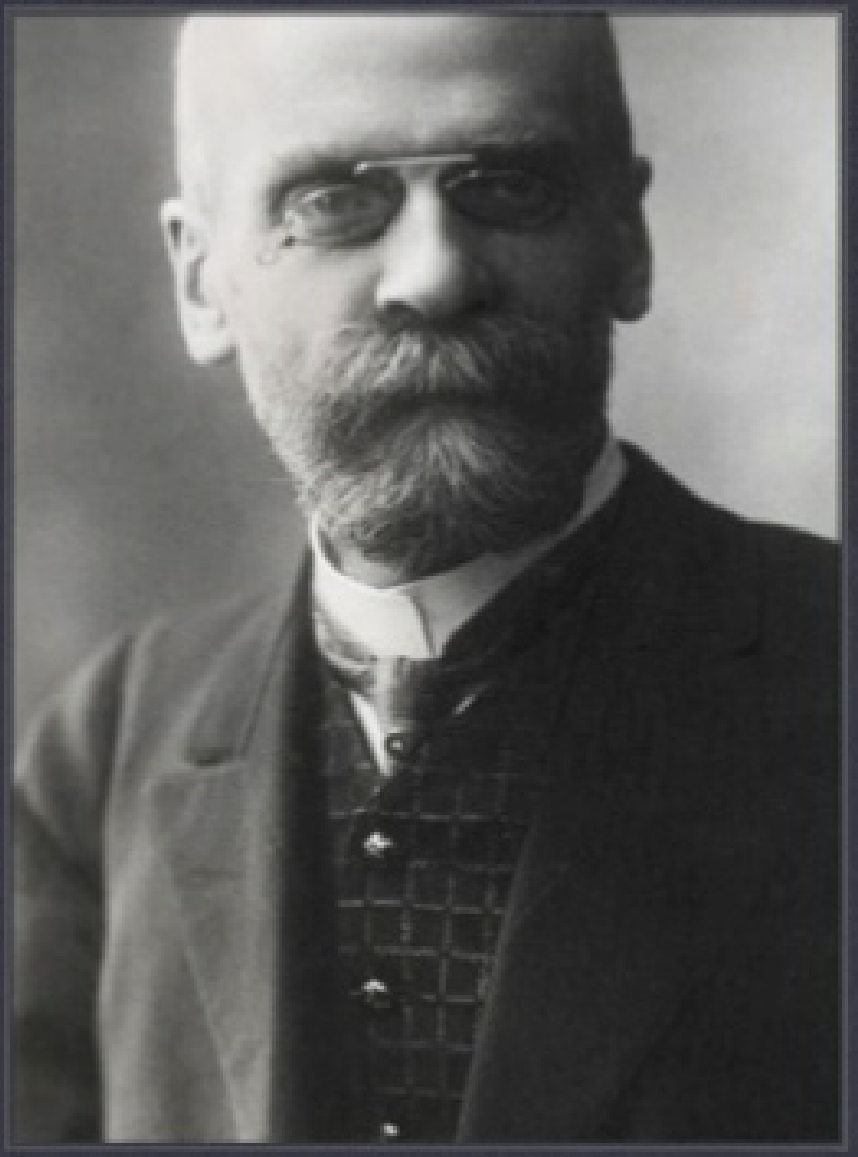
Câmara dos Deputados
Comissão de Ciência, Tecnologia e Informática

Audiência Pública

Abuso e Exploração Sexual de Crianças e Adolescentes na Internet

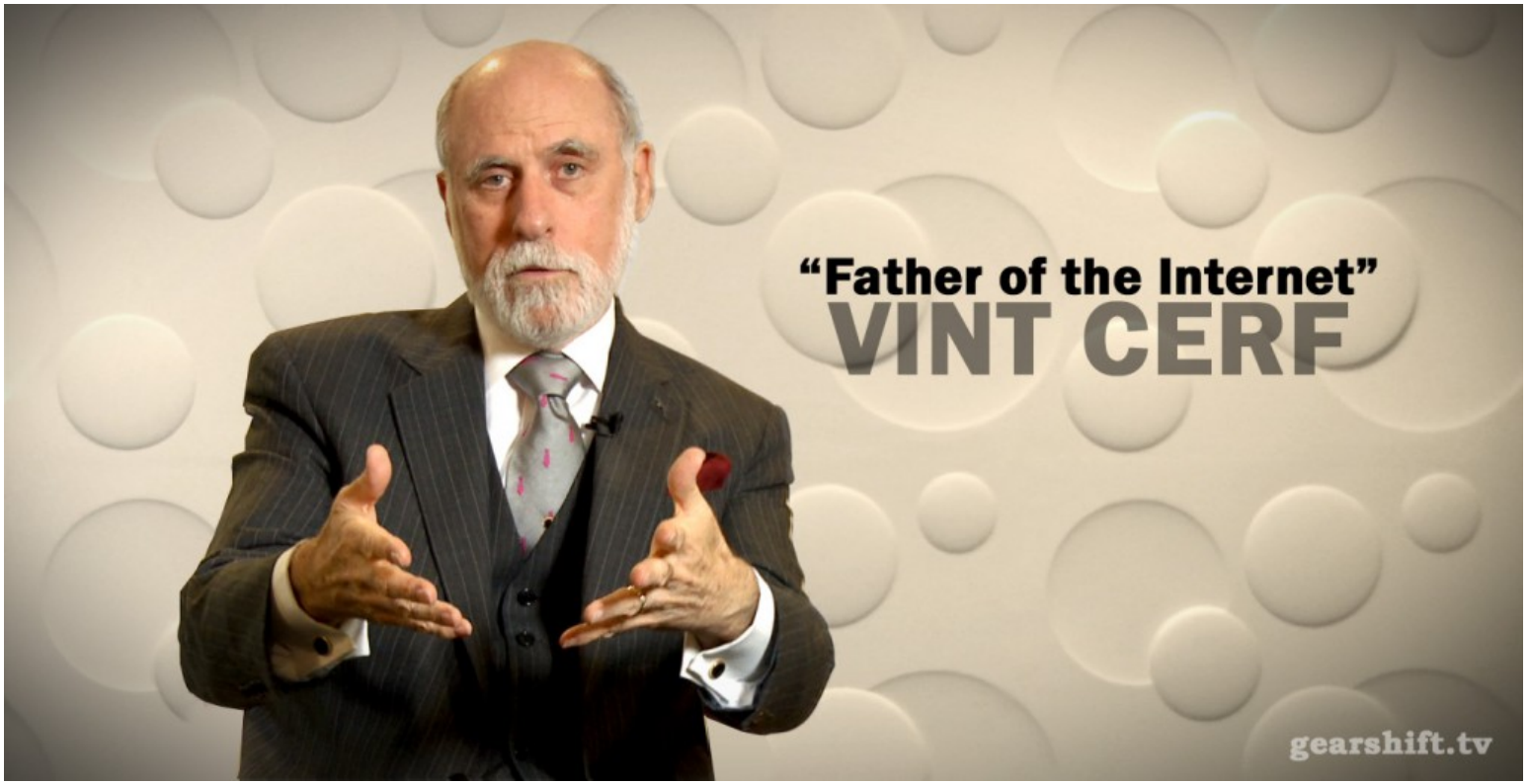
Prof. Thiago Tavares Nunes de Oliveira
Presidente da SaferNet Brasil

Onde houver sociedade, haverá crime



EMILE DURKHEIM

1858-1917



“The internet is a reflection of our society and that mirror is going to be reflecting what we see. If we do not like what we see in that mirror the problem is not to fix the mirror, we have to fix society.”

Vint Cerf

“A internet é um reflexo da nossa sociedade e esse espelho vai refletir o que vemos. Se não gostamos do que vemos nesse espelho, o problema não é consertar o espelho, temos de consertar a sociedade.”

Vint Cerf

Fonte dos dados:

- IPEA, Atlas de Violência
- UNODC Statistics
- Eurostat, Crime and criminal justice statistics
- FBI, Criminal Justice Information Services

Endereço do mapa: https://maps.blueshift.io/homicides-by-country


9:42 AM
Tuesday
9
Calendar
Photos
Maps
Weather
Notes
Settings
Mail
Safari

Poder público será responsável por bloqueio de celulares em presídios, determina projeto

Da Redação | 05/12/2017, 13h25 – ATUALIZADO EM 05/12/2017, 16h34

Geraldo Magela/Agência Senado

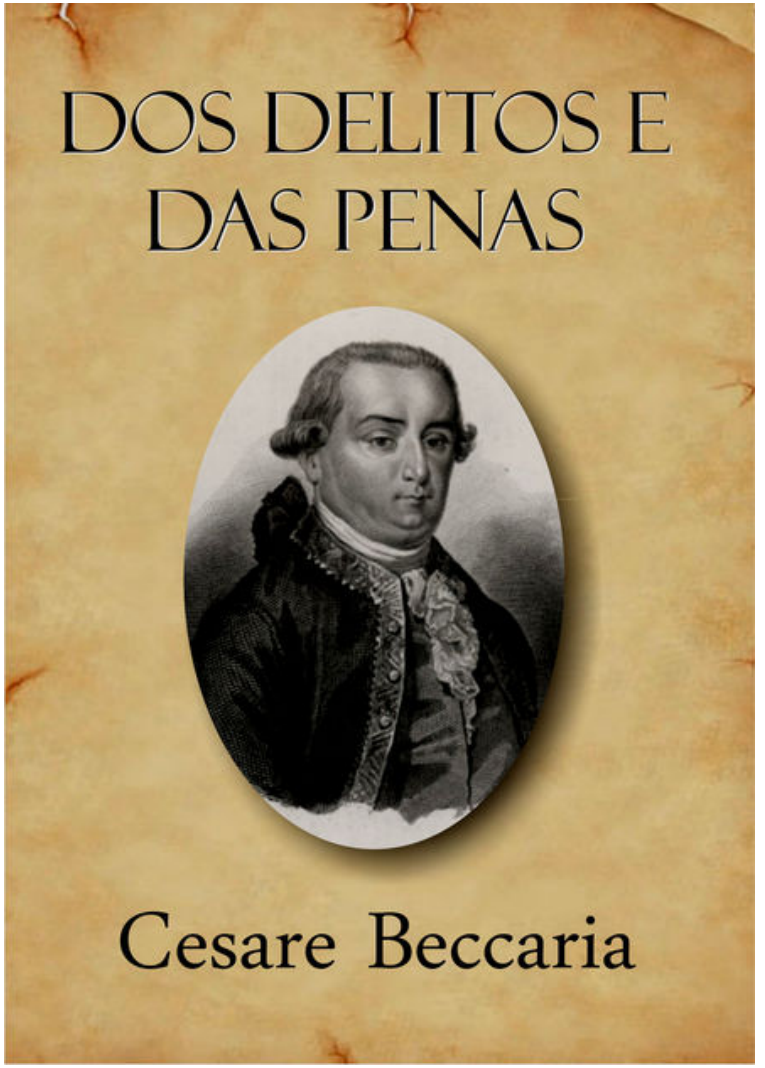
Projeto que repassa ao poder público responsabilidade de bloquear o sinal de celular nos presídios foi aprovado nesta terça-feira (5) pela Comissão de Assuntos Econômicos (CAE). A proposta, que terá votação final na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT), é um

Saiba mais

CAE aprova projeto que destina verbas do Funpen

"É melhor prevenir os crimes do que ter de puní-los. O meio mais seguro, mas ao mesmo tempo mais difícil, de tornar os homens menos inclinados a praticar o mal é aperfeiçoar a educação"

In: **BECCARIA, Cesare Bonesana*. Dei delitti e delle pene*: Milão, 1764*.***




Safer
net


A SAFERNET DEFENDE
DIREITOS HUMANOS
E LIBERDADES
NA INTERNET HÁ 11 ANOS

Educação

A educação promove o conhecimento.

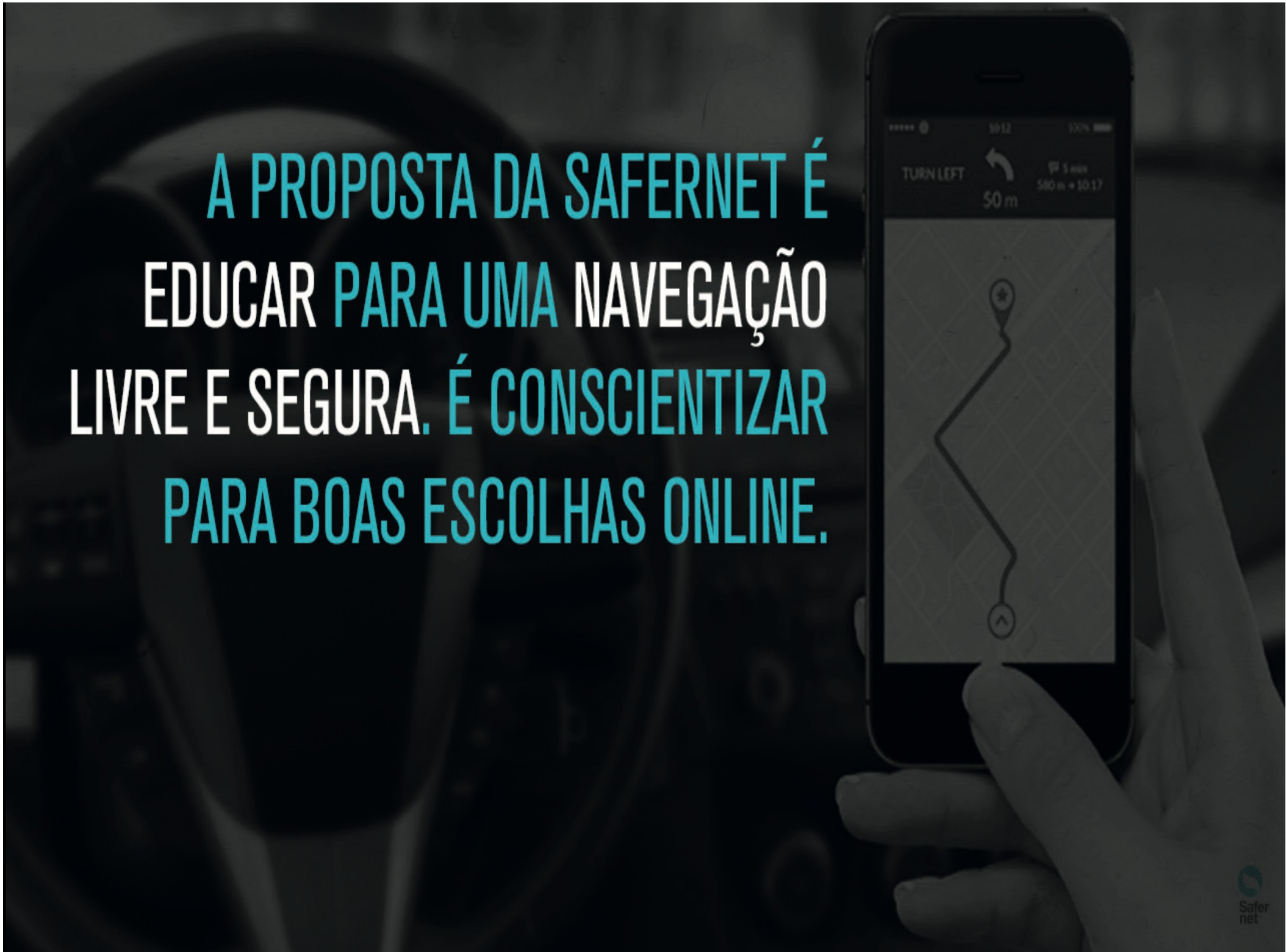
O conhecimento proporciona escolhas.

Quem tem escolhas tem liberdade para optar .

Navegar com segurança é navegar com liberdades.

É fazer boas escolhas online.


LIBERDADE + CONHECIMENTO =
CAPACIDADE PARA BOAS ESCOLHAS
Safer net


A PROPOSTA DA SAFERNET É
EDUCAR PARA UMA NAVEGAÇÃO
LIVRE E SEGURA. É CONSCIENTIZAR
PARA BOAS ESCOLHAS ONLINE.
TURN LEFT
50 m
Safer net

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES

INHOPE

ins@fe

Child Helpline International

Safer net

hotline

SELECIONE ABAIXO O TEMA A SER TRATADO

- pornografia infantil
- racismo
- apologia e incitação a crimes contra a vida
- xenofobia
- neo nazismo
- maus tratos contra animais
- intolerância religiosa
- homofobia
- tráfico de pessoas

URL do site

Comentário

Denunciar

SELECIONE O TEMA AO LADO

Selecione o tema ao lado

O QUE É O HOTLINE?

A SaferNet Brasil oferece um serviço de recebimento de denúncias anônimas de crimes e violações contra os Direitos Humanos na Internet, contanto com procedimentos efetivos e transparentes para lidar com as denúncias. Além disso, contamos com suporte governamental, parcerias com a iniciativa privada, autoridades policiais e judiciais, além, é claro, de você usuário da Internet. Caso encontre imagens, vídeos, textos, músicas ou qualquer tipo de material que seja atentatório aos Direitos Humanos, faça a sua denúncia.

ACOMPANHE SUA DENÚNCIA

Protocolo da denúncia:

Compartilhar

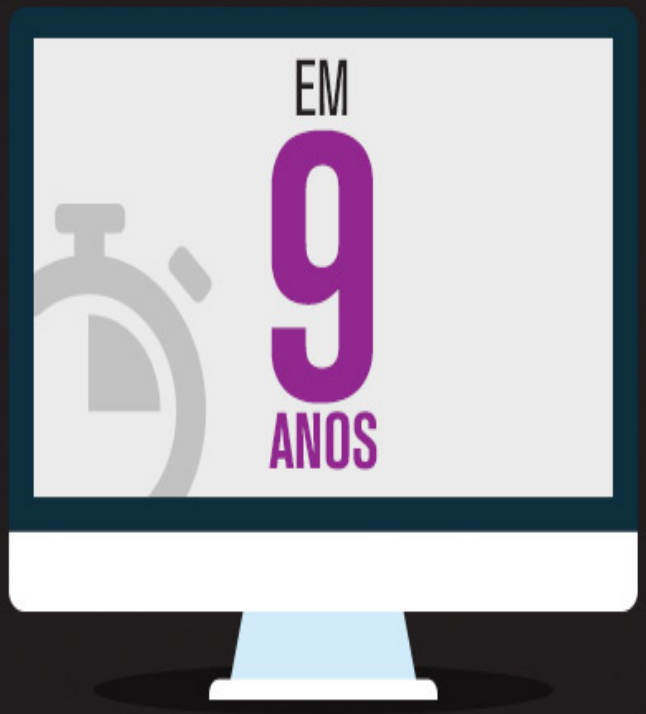
Safer net

hotline

3.606.419

DENÚNCIAS ANÔNIMAS

RECEBIDAS DO CANAL DE DENÚNCIA



585.778

PÁGINAS (URLS) DISTINTAS

9
IDIOMAS

72.739
HOSTS DIFERENTES

41.354
NÚMEROS IPS DISTINTOS

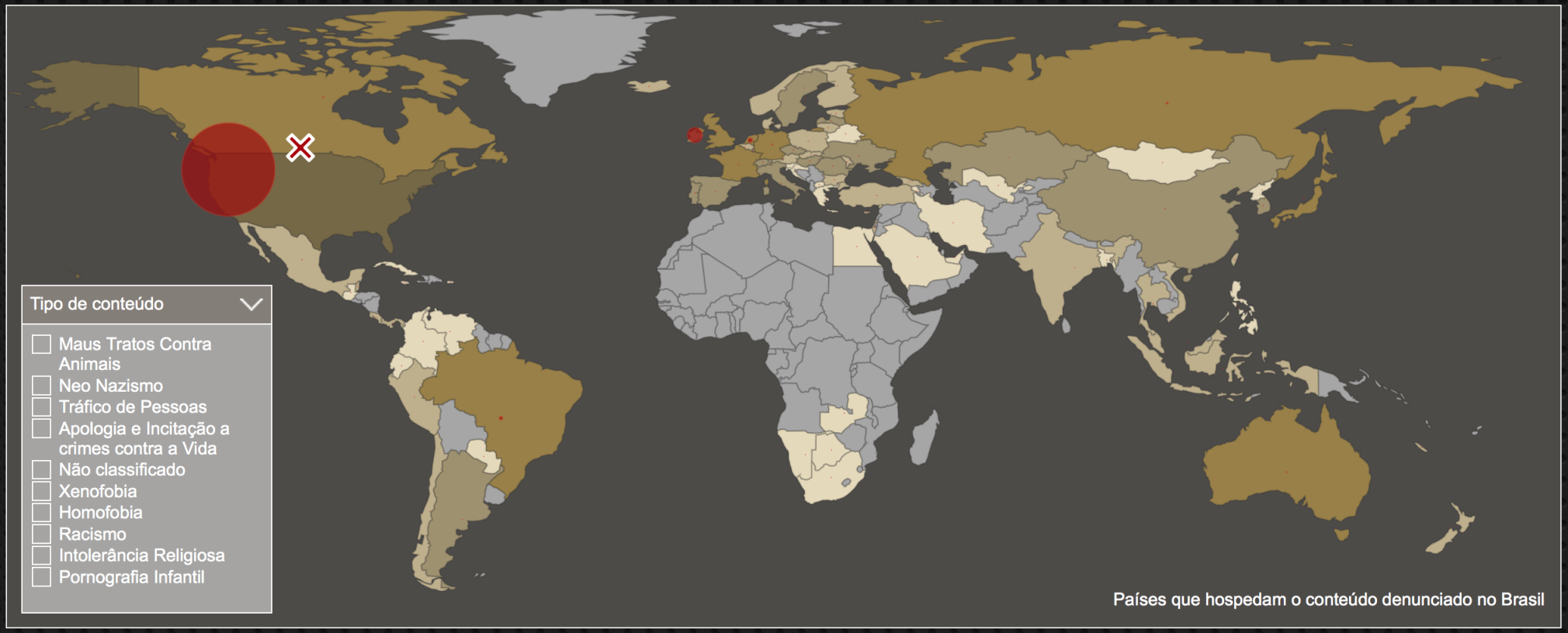
96
PAÍSES

5
CONTINENTES

Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos

COMO UTILIZAR ESTE MAPA?

Em **11 anos**, a Central de Denúncias recebeu e processou **3.861.707** denúncias anônimas envolvendo **668.288** páginas (URLs) distintas (das quais **229.359** foram removidas) escritas em **9 idiomas** e hospedadas em **86.143** hosts diferentes, conectados à Internet através de **50.405** números IPs distintos, atribuídos para **98** países em **5** continentes. As denúncias foram registradas pela população através dos **7** hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos. Saiba mais sobre este projeto!



ZOOM DO MAPA

ESCALA DA BOLHA

LINHA DO TEMPO

2006 a 2016

http://denuncie.org.br/indicadores

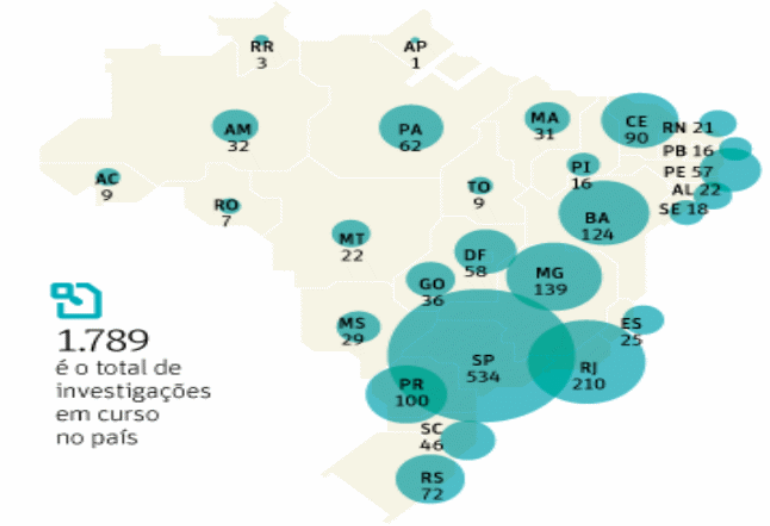
Cooperação Multisetorial

Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

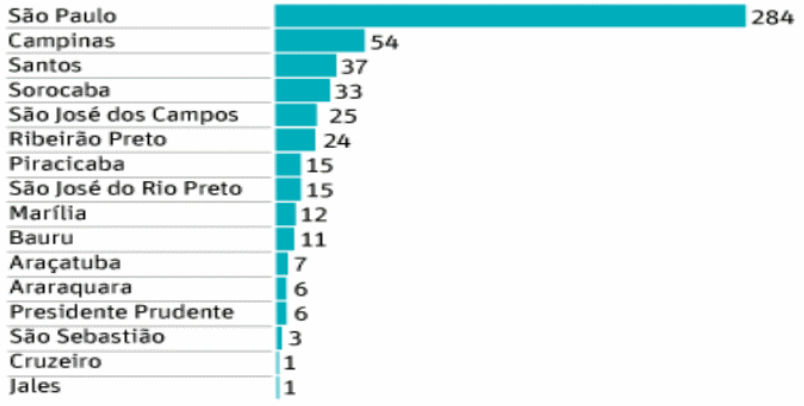
MAPA DAS AÇÕES CONTRA A PORNOGRAFIA INFANTIL

Prisões em flagrante na última década

Ranking nacional de investigações em curso



Unidades da PG com maior número de investigações em SP



Fonte: Polícia Federal

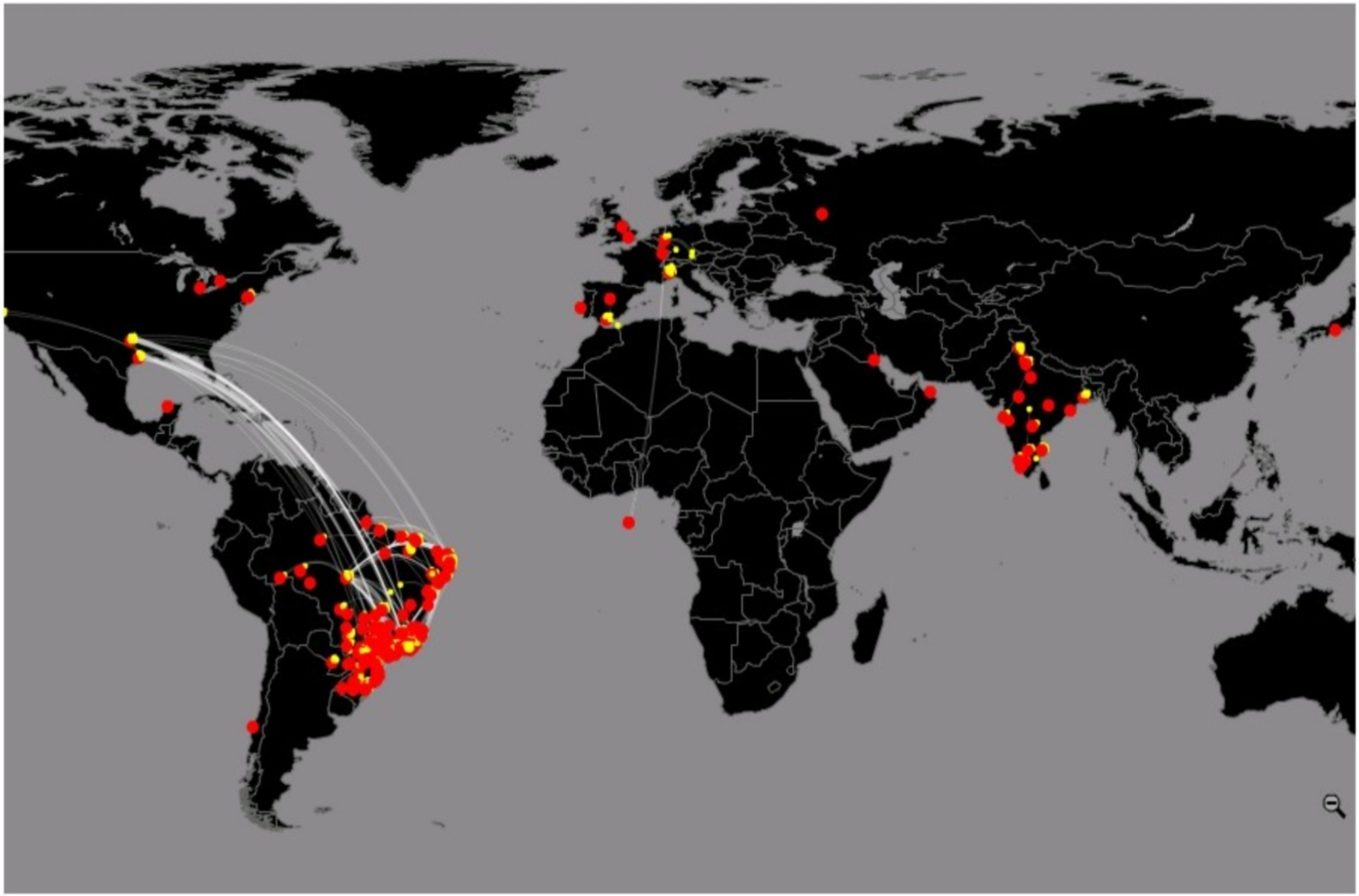
2014: 126 prisões em flagrante

2015: 185 prisões e 1496 IPLs instaurados

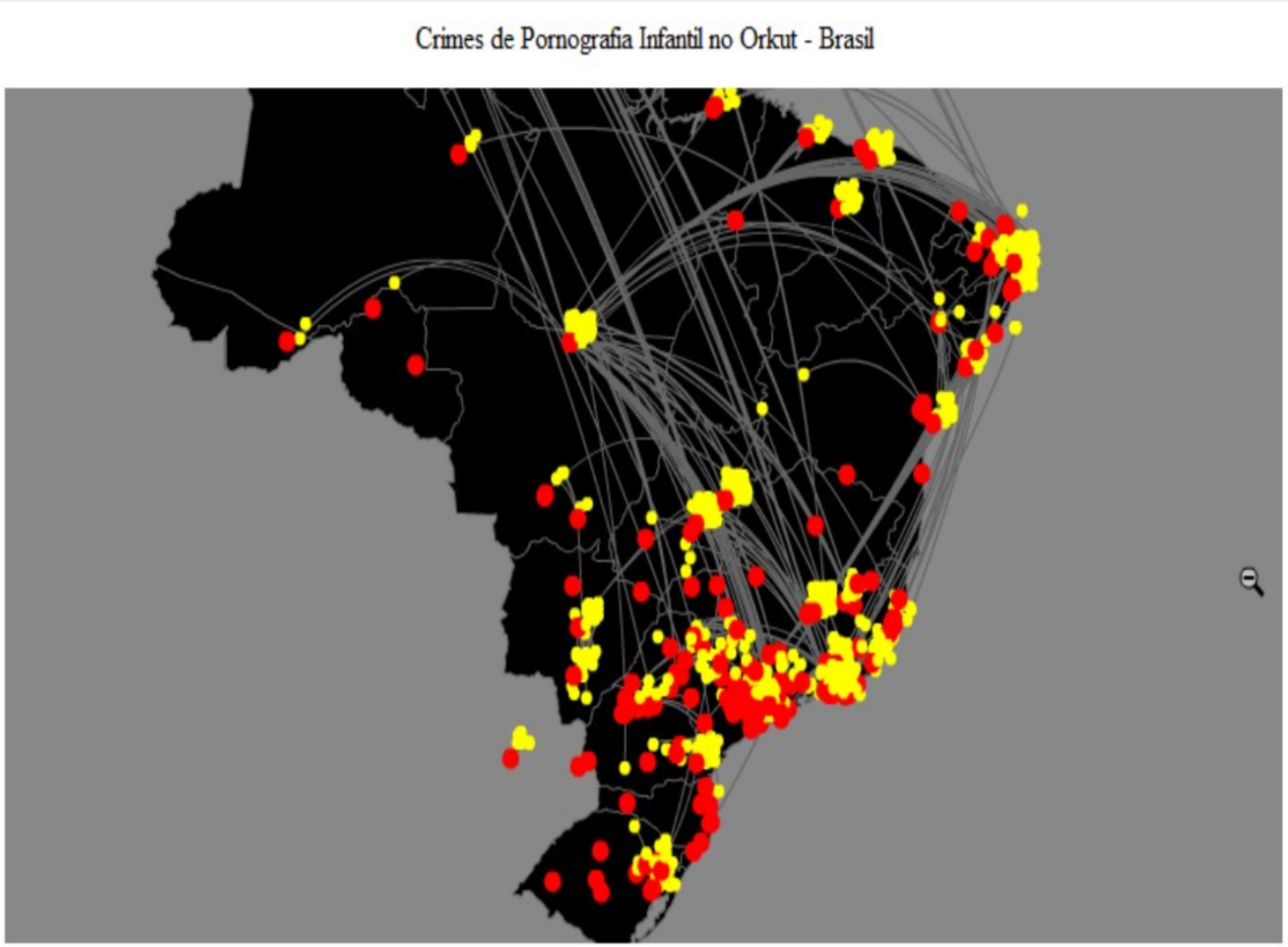
2016: 128 prisões em flagrante

2017: 156 prisões em flagrante (até out/2017)

Investigação 01 (iniciada em maio de 2008) – 1263 conexões em 12 países (874 no Brasil) – 300 agressores sexuais investigados



643 perfis investigados na Op. Turko



#INDICADORESHELPLINE

hotline
helpline

2007 / 2016

TOTAL DE ATENDIMENTO

13.268
PESSOAS ATENDIDAS

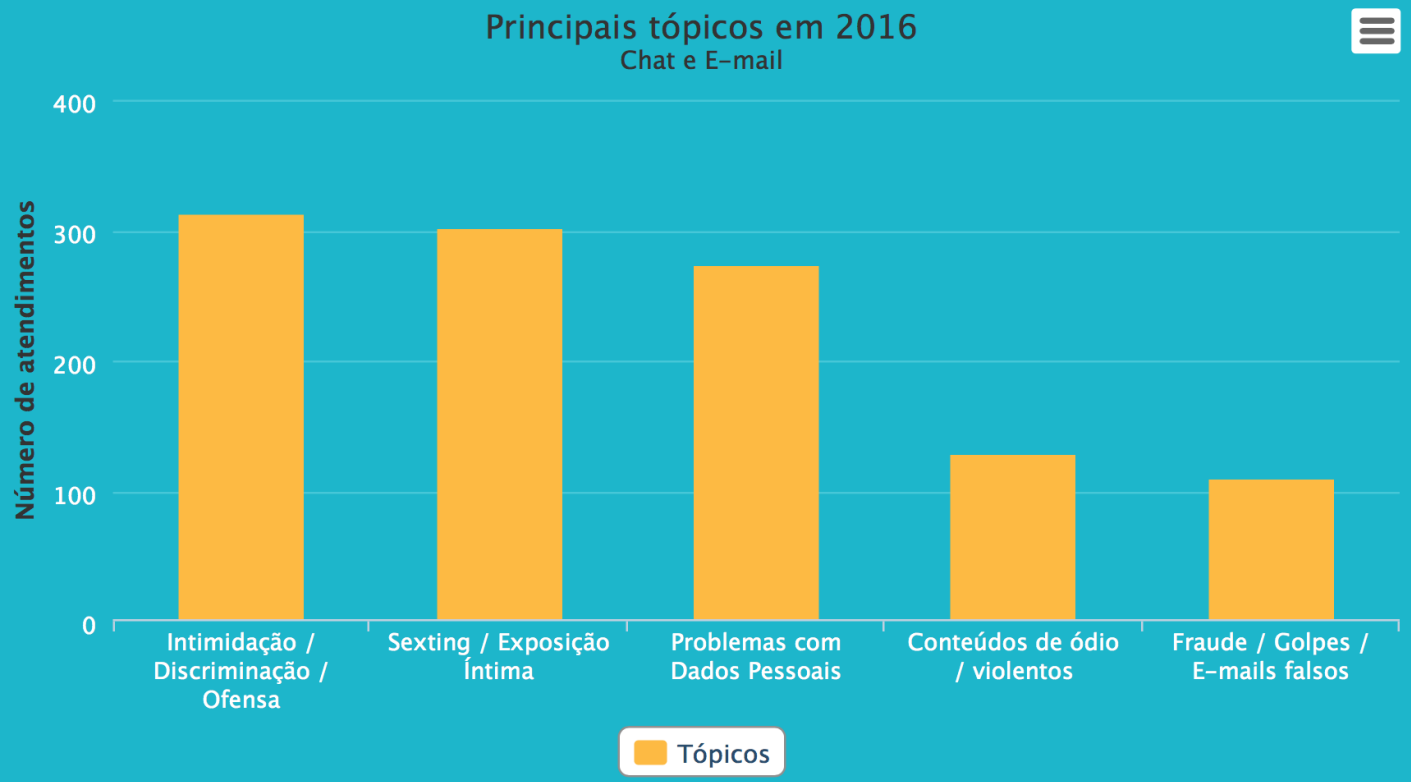
26
ESTADOS

1.402 CRIANÇAS E ADOLESCENTES
1.538 PAIS E EDUCADORES
9.893 OUTROS ADULTOS

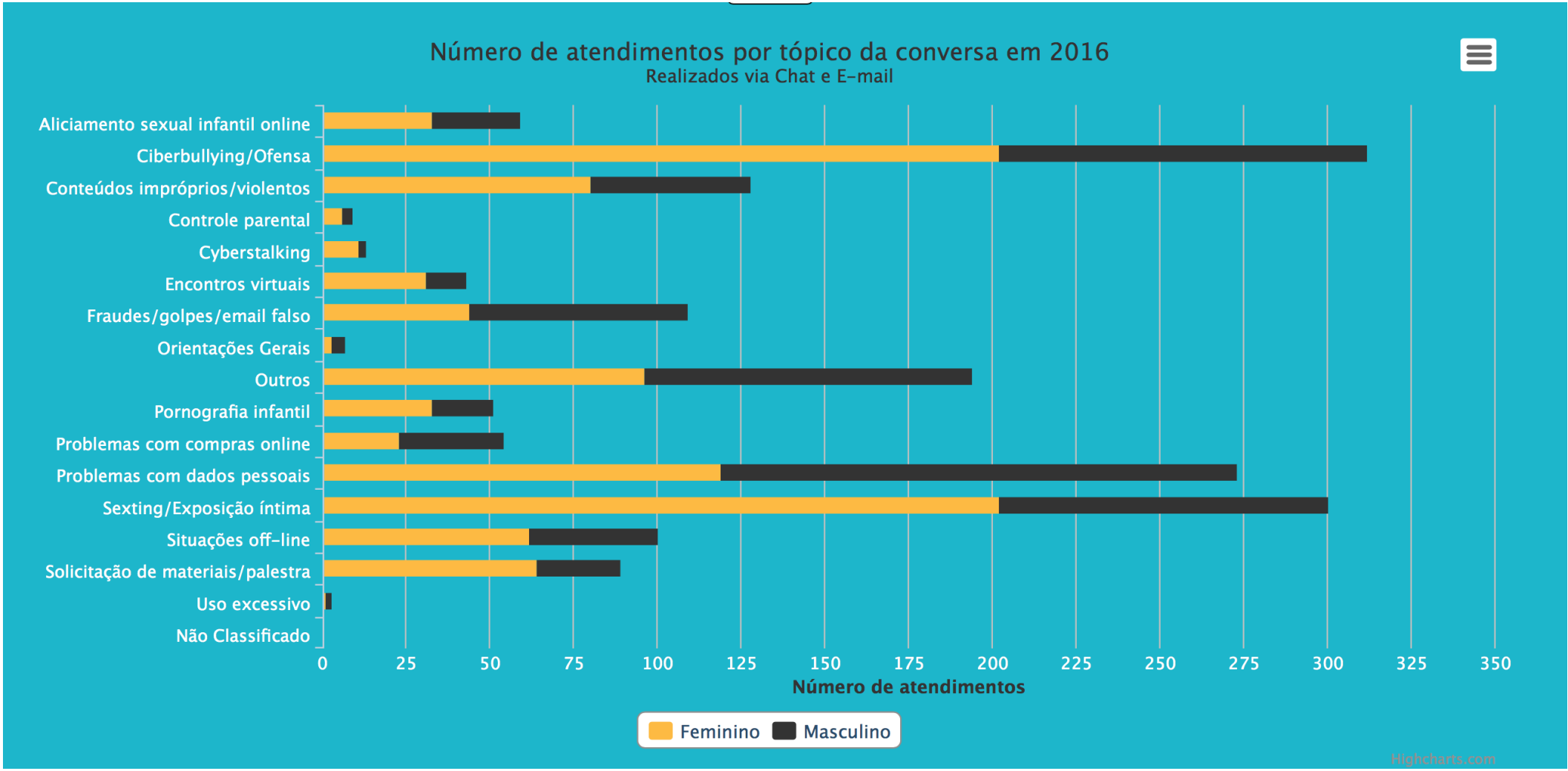
① AS PRINCIPAIS VIOLAÇÕES PARA AS QUAIS OS INTERNAUTAS BRASILEIROS PEDEM AJUDA

http://helpline.org.br/indicadores

1 AS PRINCIPAIS VIOLAÇÕES PARA AS QUAIS OS INTERNAUTAS BRASILEIROS PEDEM AJUDA



http://helpline.org.br/indicadores



http://helpline.org.br/indicadores

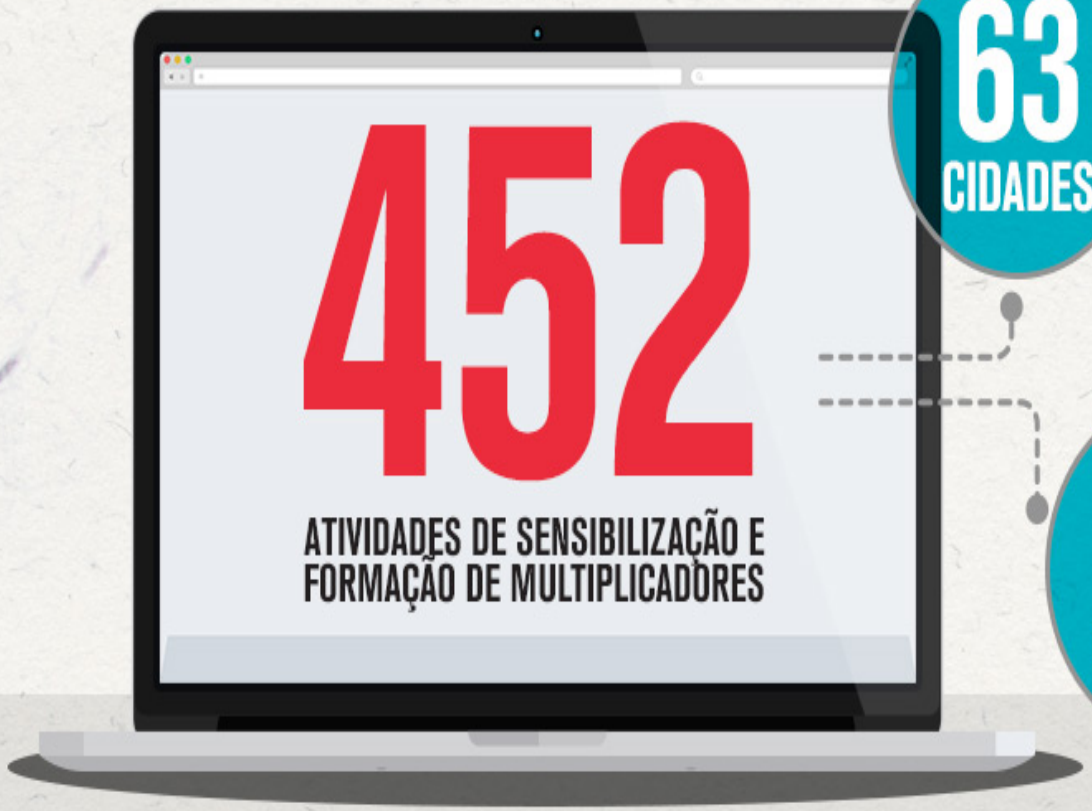
helpline

DIA INTERNET SEGURA

15.162
CRIANÇAS E ADOLESCENTES

18.234
PAIS E EDUCADORES

865
AUTORIDADES



452
ATIVIDADES DE SENSIBILIZAÇÃO E FORMAÇÃO DE MULTIPLICADORES

63
CIDADES

21
ESTADOS

MAIS DE
115 MIL
PESSOAS
EM MAIS DE
460
EVENTOS
EM
63
CIDADES
EM TODO
O BRASIL!

Safer net

Ciclo de Oficinas

Segurança, ética e cidadania na Internet:
educando para boas escolhas online

Princípios
Decálogo
CGI.Br

Liberdade, Privacidade
e Direitos Humanos

3.861.707
dénúncias recebidas e
processadas pela Safernet

13.268 atendimentos realizados
no canal de ajuda da Safernet

20% dos usuários
entre 9 e 17 anos já se
sentiram ofendidos online
CETIC.br/NIC.br

65% dos professores apontaram que os
alunos NÃO recebem instruções sobre como
usar a Internet com segurança na sua escolas.
CETIC.br/NIC.br

O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a ***capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet*** *como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.*

Art. 26 - Marco Civil da Internet

datasafer

INDICADORES CENTRAL DE DENÚNCIAS CANAL DE ATENDIMENTO

oficinas
hotline
helpline

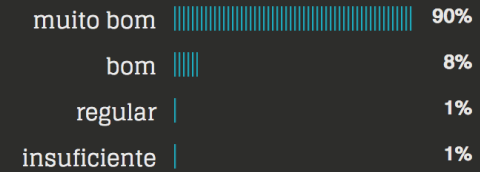
2015
2016
2017
todos

EM 3 ANOS, 26 OFICINAS CAPACITARAM DIRETAMENTE 3.832 EDUCADORES DE 297 MUNICÍPIOS EM 22 UFS, E BENEFICIARAM 985.988 ALUNOS EM 673 ATIVIDADES DE MULTIPLICAÇÃO NAS ESCOLAS/INSTITUIÇÕES MOBILIZADAS, GERANDO MAIS DE 200 NOTÍCIAS NA IMPRENSA LOCAL E NACIONAL

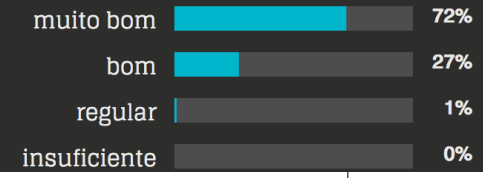
SITE DO PROJETO

BRASIL

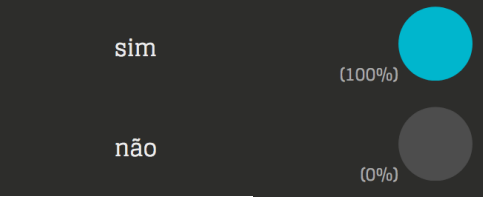
COMO AVALIA A RELEVÂNCIA DO TEMA E DOS CONTEÚDOS?



APRENDIZAGEM SOBRE O TEMA



VOCÊ RECOMENDARIA ESTA ATIVIDADE?



NOTÍCIAS

Escolas treinam professores para ensinar alunos sobre perigos da web

Fonte: Bom Dia Brasil - Rede Globo

Realização

Safernet

PFDC Procuradoria Federal dos Direitos do Cidadão

MPF Ministério Público Federal

Patrocínio

nic.br Núcleo de Informação e Coordenação do Ponto BR

20 anos cgi.br Comitê Gestor da Internet no Brasil

Apoio

unicef

Saiba mais:

http://mapa.safernet.org.br

6 DE JULHO DE 2015 ÀS 15H56

MPF/RS e Safernet realizam oficina de proteção à infância e à adolescência na Web

Encontro ocorre nesta terça-feira, 7 de julho, na Capital

Educadores, coordenadores pedagógicos ou tecnológicos e representantes da área de ensino estarão reunidos nesta terça-feira (7/07), na Capital, para discutir a "Segurança, ética e cidadania na Internet: educando para boas escolhas online".

A oficina é uma iniciativa nacional do Ministério Público Federal (MPF), por meio da sua 2ª Câmara de Coordenação e Revisão – que trata da atuação criminal e abriga o Grupo de Trabalho de Enfrentamento aos Crimes Cibernéticos – e da Procuradoria Federal dos Direitos do Cidadão em conjunto com a ONG Safernet Brasil e o Comitê Gestor da Internet do Brasil – CGI.br.

Considerei que a metodologia utilizada durante toda a atividade foi muito significativa, a forma como os temas foram abordados, de maneira didática e com exemplos comuns do dia a dia.

Gostei muito e me senti na responsabilidade de multiplicar.
Coloquei em prática já no dia seguinte para os colegas de trabalho do setor que trabalho.

Uma nova abordagem com uma nova visão, fazendo entender que as crianças e jovens podem utilizar a Internet, mas de modo crítico e seguro, preparando os usuários para os possíveis perigos da navegação.


Omega


Segurança
SaferNet
Omega


SEM
VA
REITOS
guais

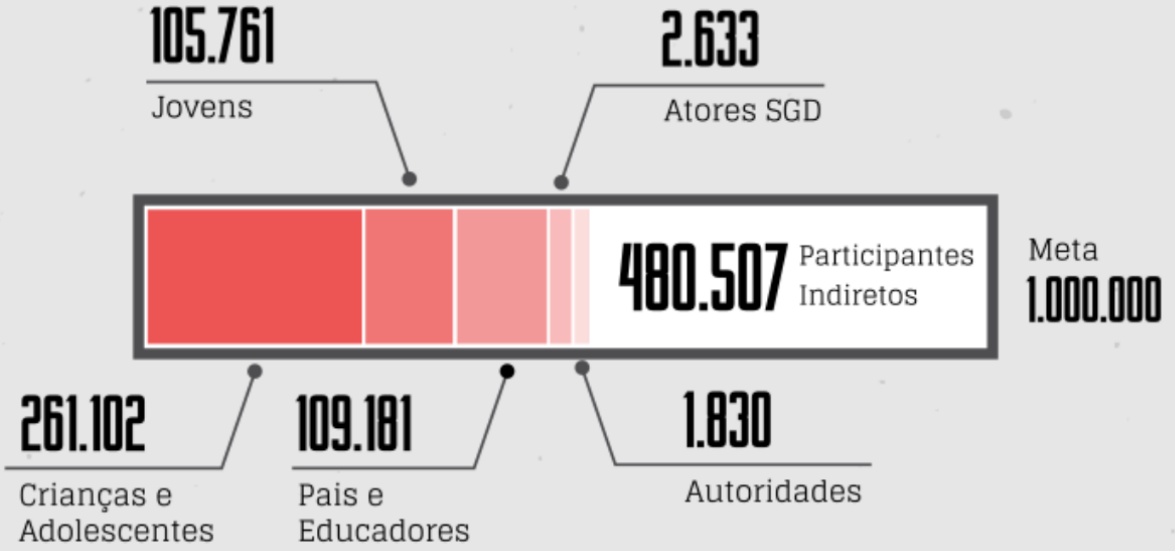
Disponível para download em: http://www.safernet.org.br/site/sid2017/recursos

Ações de multiplicadores:

532 Atividades de multiplicadores

194 Municípios diferentes

40.356 Itens enviados

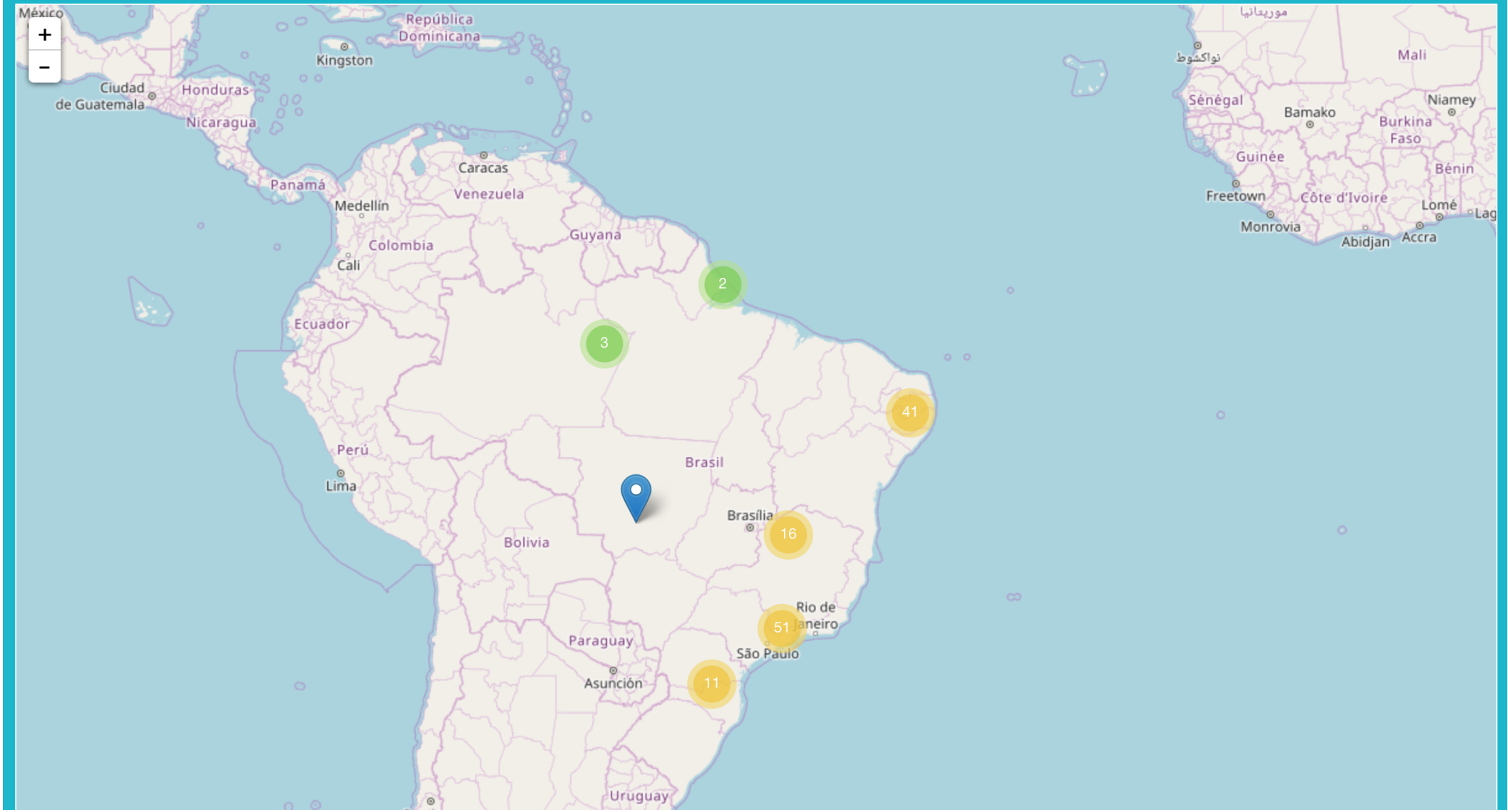


www.diadainternetsegura.org.br


PARCEIROS

Este mapa contém as **125** atividades que foram programadas em todo o país em torno do Dia da Internet Segura 2017, contemplando um público de **69643** pessoas em **83** municípios de **18** Estados brasileiros. Cadastre a sua atividade através do link acima.

Confira a íntegra dos vídeos do Evento HUB que ocorreu no dia 07/02 em São Paulo - SP.



ALICIAMENTO - **CAMPANHAS**

SEXTING - O QUE ACONTECE

Página inicial » Geral

Compartilhar fotos íntimas na internet é crime, alerta polícia

Autoridades usam os artigos do Código Penal para fixar as penas

Tweetar 2 | Curtir | Compartilhar 40 | 0 | corrigir texto

...ácil e ágil compartilhar informações, pensamentos...
...ntade. Basta um clique. O cuidado com o que ...
...nal, divulgar fotos sem o consentimento da pess...
...es são vítimas da rede. Eles tiveram suas intimida...

NOTÍCIAS | MULTIMÍDIA | BLOGS

Adolescente é exposta no Facebook por ex-namorado

Do total de crimes por injúria e difamação contra mulher... DDM de Araraquara, 40% são virtuais

09h06 | 06/05/2014

Araraquara.com / Da reportagem

compartilhar 0 | tweetar 0 | 0

...ra a delegada da Mulher, Meirelene de Castro
...drigues, o problema é o usuários da internet
...editar que isso nunca aconteceria com ele
...teus Rigola/Tribuna Impressa)

A exposição de fotos e vídeos íntimos na internet pelo ex-namorado de uma adolescente de 14 anos em Araraquara chama a atenção sobre até que ponto os usuários da rede devem se expor e os cuidados que devem tomar.

Inconformado com o fim do namoro um rapaz, de 19 anos, colocou as imagens íntimas da garota no Facebook. A família dela pretende processá-lo. (leia mais abaixo)

Segundo levantamento da DDM (Delegacia de Defesa da Mulher), somente nos quatro primeiros meses de 2014, 110 casos de injúria e difamação envolvendo mulheres foram

...trados em Araraquara.
...e total, 40%, ou seja 44, foram praticados pela internet, o que resulta numa média de 11 casos por
...u um a cada três dias.

...do a delegada da Mulher, Meirelene de Ca...
"Quando assu...

G1 | Na TV | Esporte | Trânsito | Aeroportos | Agenda de shows | VC no G1

18/11/2013 15h06 - Atualizado em 18/11/2013 16h20

Jovem denuncia ex-namorado por ameaça e desabafa contra foto nua

Thamiris Sato diz que pensou em se matar por causa do constrangimento. Ex-namorado búlgaro citado não foi localizado para comentar o tema.

Tweet

Kleber Tomaz
Do G1 São Paulo

Uma jovem de 21 anos, aluna de letras da Universidade de **São Paulo** (USP), procurou a internet e a Polícia Civil de São Paulo para denunciar o ex-namorado, um búlgaro de 26 anos, também estudante do mesmo curso na mesma universidade, por postar fotos íntimas dela no Facebook e de ameaçá-la de morte após o fim do namoro.

Em entrevista nesta segunda-feira (18) ao **G1**, a Thamiris Natalie Mayumi Sato, estudante de ...versidade de São Paulo, falou que ...ão, em 31

G1 | Na TV | Esporte | Trânsito | Aeroportos | Agenda de shows | VC no G1

23/10/2013 12h30 - Atualizado em 23/10/2013 16h29

'Não me arrependo porque fiz por amor', diz garota sobre vídeo de sexo

Jovem de 19 anos teve imagens íntimas divulgadas nas redes sociais. Em entrevista exclusiva, ela desabafa: 'Queria ter minha vida de volta'.

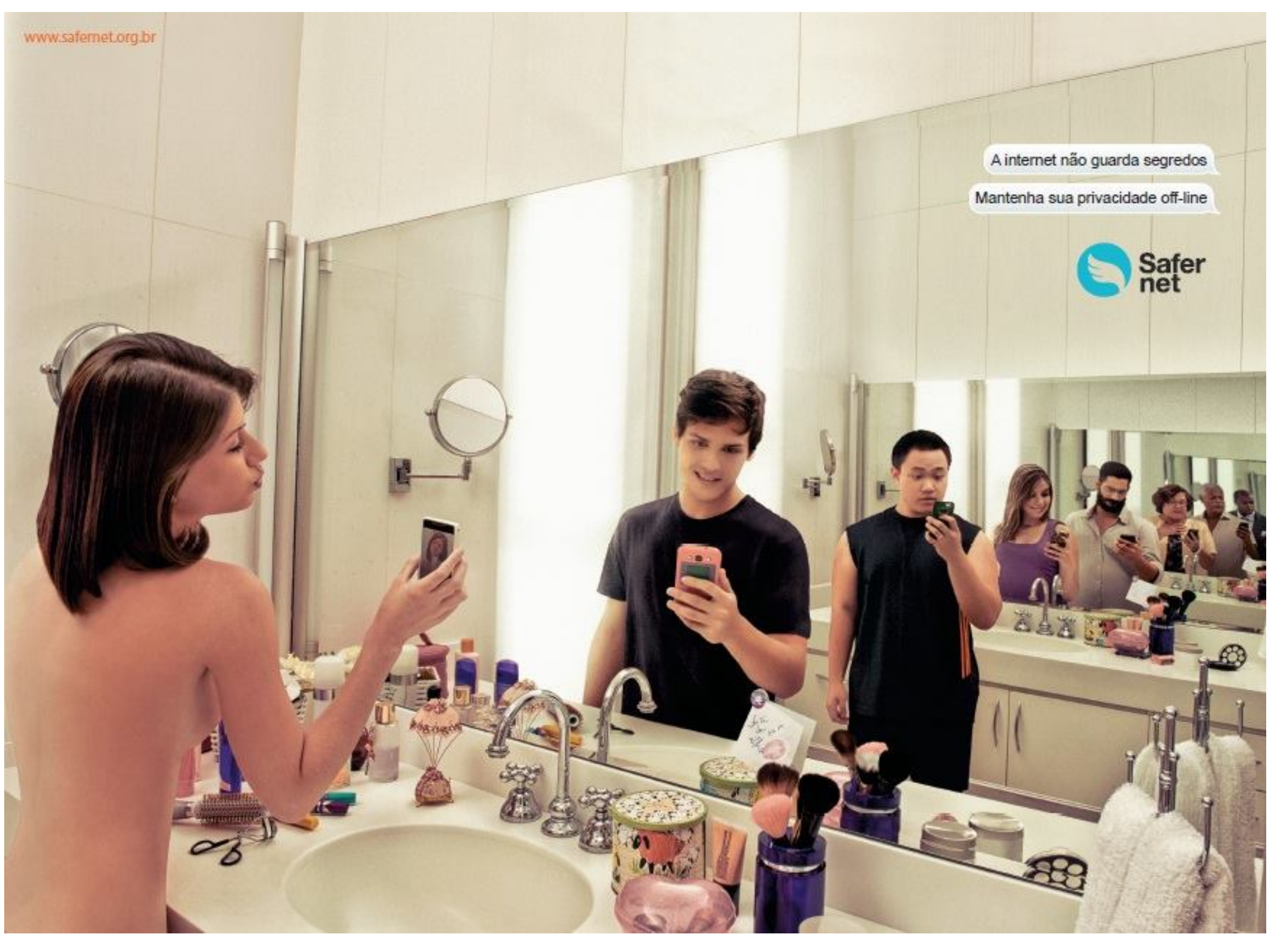
Paula Resende
Do G1 GO

Tweet 336 | Recomendar 10 mil

A estudante de 19 anos que teve vídeos íntimos divulgados em um aplicativo de celular e nas redes sociais diz que sua vida "virou um inferno". Parou de estudar e de trabalhar desde que o caso ganhou repercussão, no início do mês. Ela só sai de casa para conversar com advogados sobre o processo que move contra o suspeito de divulgar as imagens, com quem a jovem diz ter se relacionado por três anos. "Não me arrependo porque fiz [o vídeo] por amor, confiava. Só que isso não deveria ter sido mostrado para ninguém", disse a jovem, em entrevista exclusiva ao **G1** e à TV Anhanguera, na manhã desta quarta-feira (23), em **Goiânia**.

...balada e com o visual diferente, para não ser ...conhecida nas ruas, ela conta que está há ...ficamente 20 dias sem sair de casa. A ...dante, que era vendedora em uma loja de ..., resolveu falar publicamente sobre o ...ue ela considerou "humilhante", porque, ... não conhecem toda a história.

Safer net


www.safernet.org.br
A internet não guarda segredos
Mantenha sua privacidade off-line
Safer net

ME MANDA NUDE, VAI...
EU NÃO MOSTRO PARA NINGUÉM

COMPARTILHAR NUDES DOS OUTROS, SEM AUTORIZAÇÃO, É CRIME.

FOI VÍTIMA? ACESSE
HELPLINE.ORG.BR

ORIENTAÇÃO PARA CRIANÇAS E ADOLESCENTES

GRATUITO E SEGURO

PSICÓLOGAS ESPECIALIZADAS

CHAT - SEG. A SEX. 14H ÀS 18H

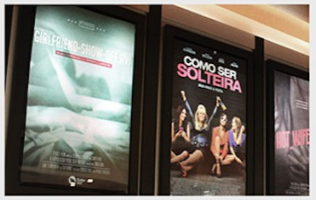
ATENDIMENTO POR E-MAIL 24H

Realização:

Safernet.org.br

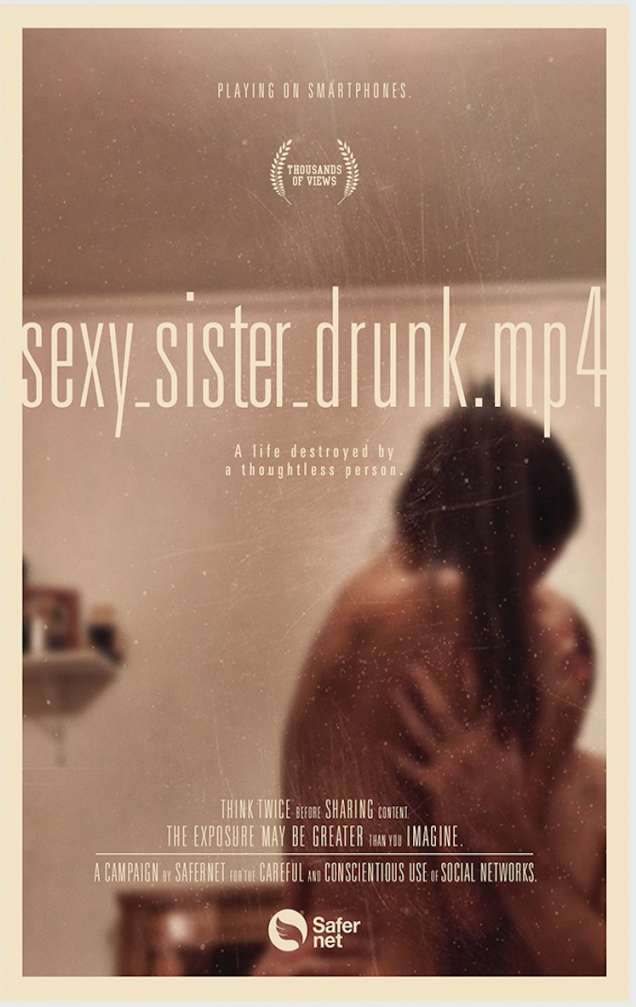
INTIMATE POSTERS

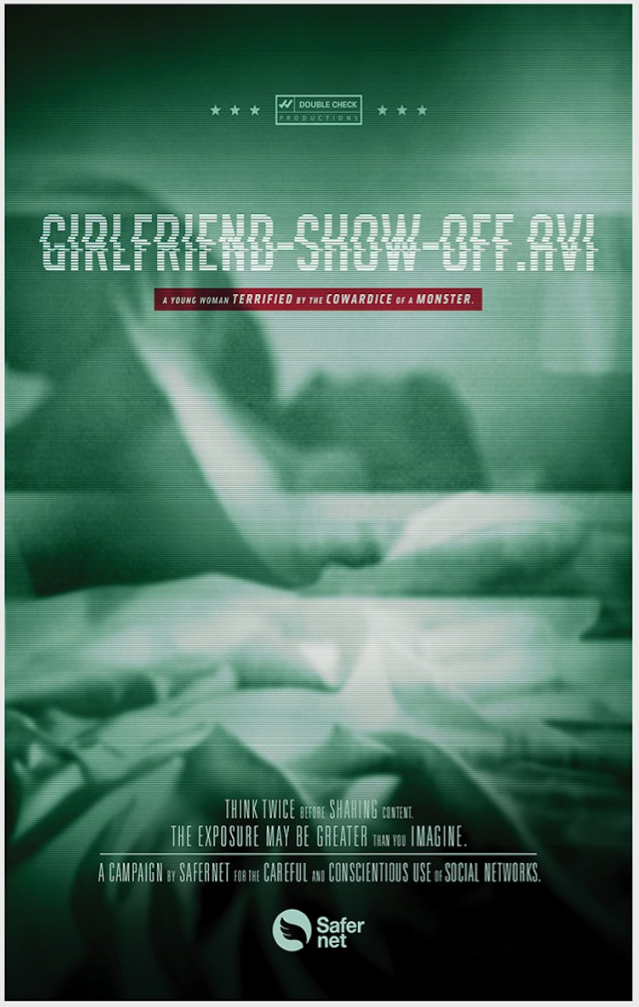
EXPOSURE MAY BE GREATER THAN YOU THINK.



PROBLEM_ The leaking of intimate videos on the internet is increasing every year. In most cases the victims are women, who end up having their lives destroyed by a reckless attitude.

IDEA_ To alert about the risks of this practice, SaferNet created an action in partnership with movie theaters where posters of fictional movies were put up alongside posters of movies playing in theaters.





Boas práticas internacionais

Defining a Hotline

A hotline is a national online resource that offers the public a way to report illegal content. Citizens are always encouraged to report suspected CSAM, which can be submitted anonymously to the hotline. Given the anonymous nature of reporting potential CSAM to hotlines, internet users are less wary of punitive action. Reports that confirm the legitimate presence of CSAM will be passed to the relevant law enforcement agency and/or Internet Service Providers(ISP). In many cases, the service provider hosting the content is then given notice to ensure rapid takedown of the material.

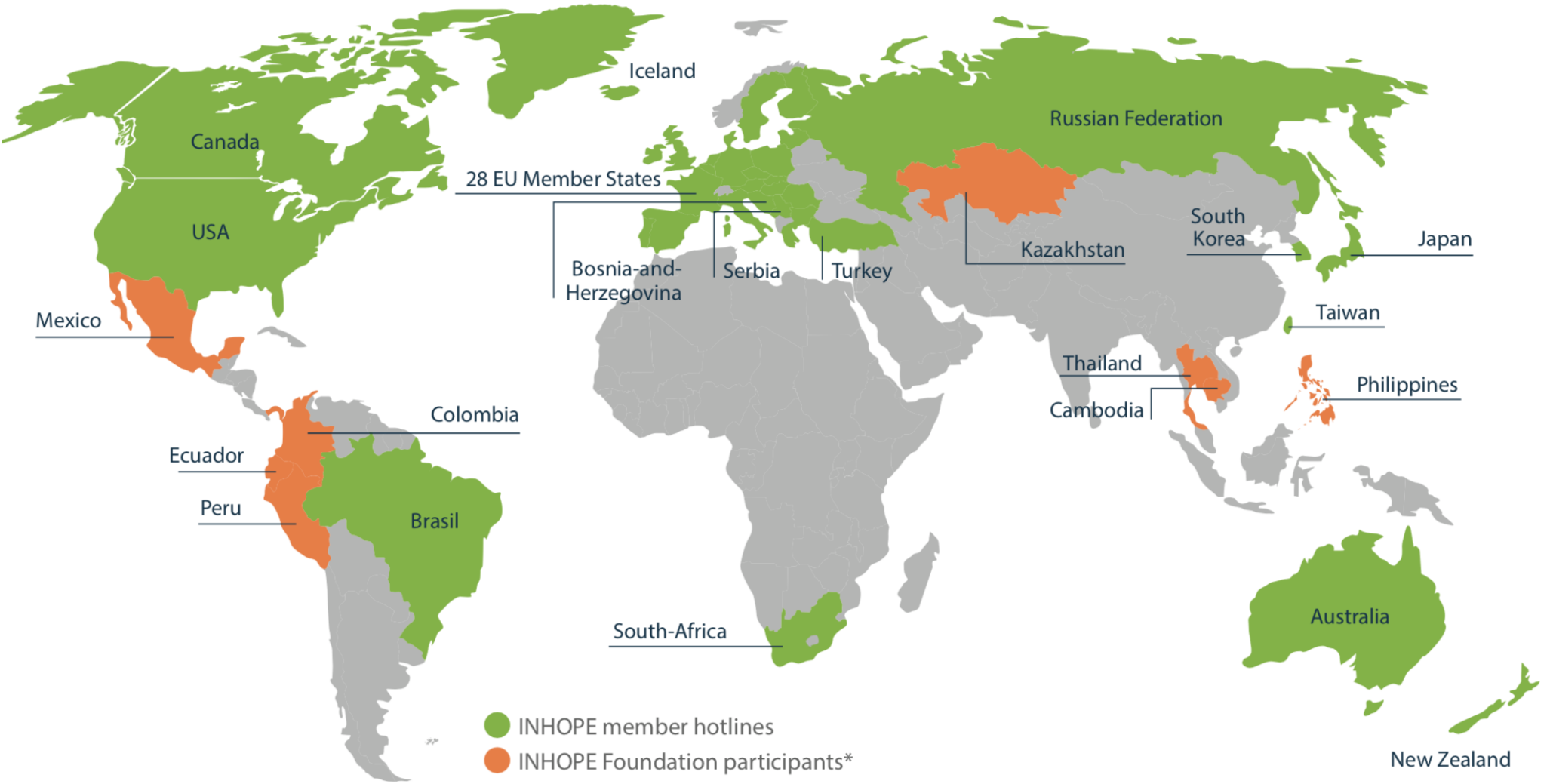
The aim of the INHOPE Hotline Network is to streamline processes for reporting illegal online content when it involves the sexual abuse or exploitation of a child. Hotlines often encourage reporting even for suspected exploitation, such as child modelling.

Hotlines are unified by their commitment to the protection of children in their country, even while facing challenges in funding and capacity. Their active collaboration to remove CSAM from the internet is vital, and it is INHOPE's priority to help them facilitate this process as rapidly and efficiently as possible.

Fonte: http://www.inhope.org/Libraries/2016/INHOPE_2016_Statistics.sflb.ashx

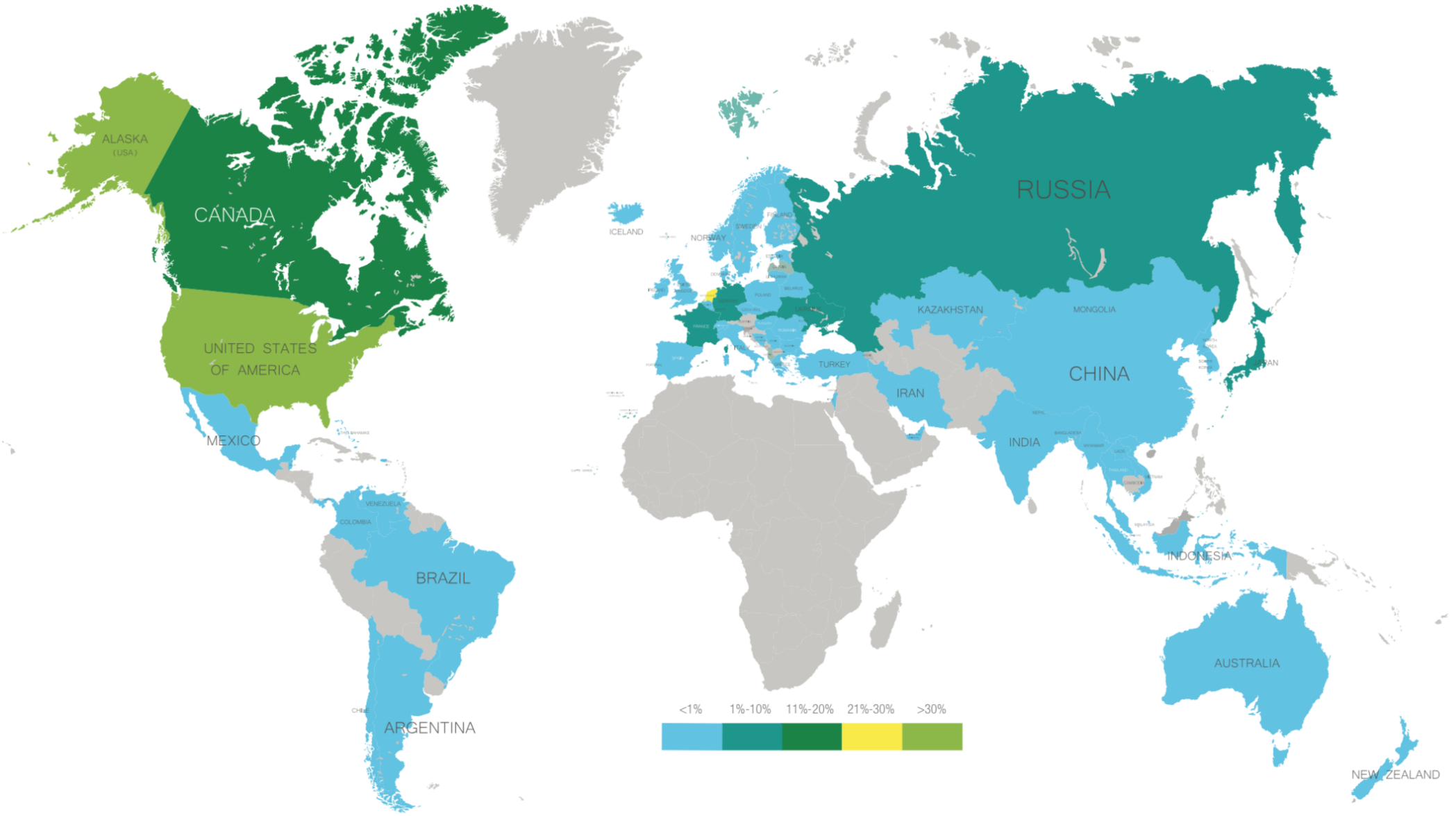
INHOPE, the global network of reporting hotlines fighting child sexual abuse material on the Internet

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE



* The INHOPE Foundation is INHOPE's charitable arm to help develop new hotlines worldwide.

2016 Global CSAM Hosting Map



Presented here is ICCAM data for the 12-month period of January 1st to December 31st 2016.

Fonte: http://www.inhope.org/Libraries/2016/INHOPE_2016_Statistics.sflb.ashx

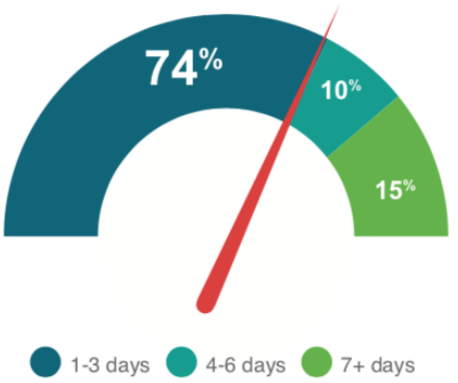
Notice and takedown timeline

Of the 38,767 total ICCAM reports both confirmed as CSAM and marked as removed by hotlines worldwide, 74% were removed within 3 working days.

Notice and takedown (NTD) refers to the number of business days between the date a hotline receives a report containing suspected CSAM, and the date a hotline analyst marks the report as Content Removed. Rapid NTD is a major weapon in combatting the spread of CSAM, disrupting the cycle of content duplication and global redistribution that results in the revictimisation of abuse victims that are shown in CSAM material. Average NTD response times have improved incrementally as technology and reporting processes have become more efficient, resulting in CSAM being removed from the internet faster than ever.

In regard to report handling via ICCAM a powerful example of this technology is hashing, which is a mathematical process of assigning computer files (images, video etc.) with a unique alphanumeric identifier. This allows files to be compared electronically with previously identified CSAM which has two main benefits – faster removal of CSAM, and support of law enforcement's efforts to identify victims and perpetrators by giving the option to focus on previously unseen CSAM.

What are the numbers showing us?

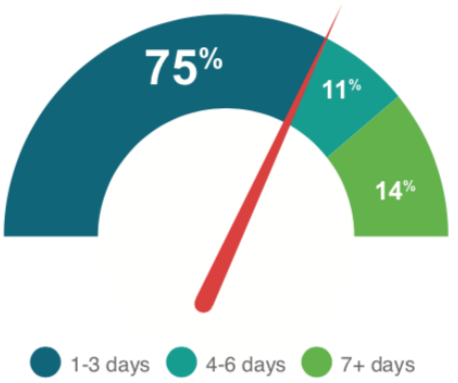


N1 = 38,767

REPORTS WORLDWIDE

74%

was removed from the Internet in less than three days.



N2 = 29,567

REPORTS IN EUROPE

75%

was removed from the Internet in less than three days.

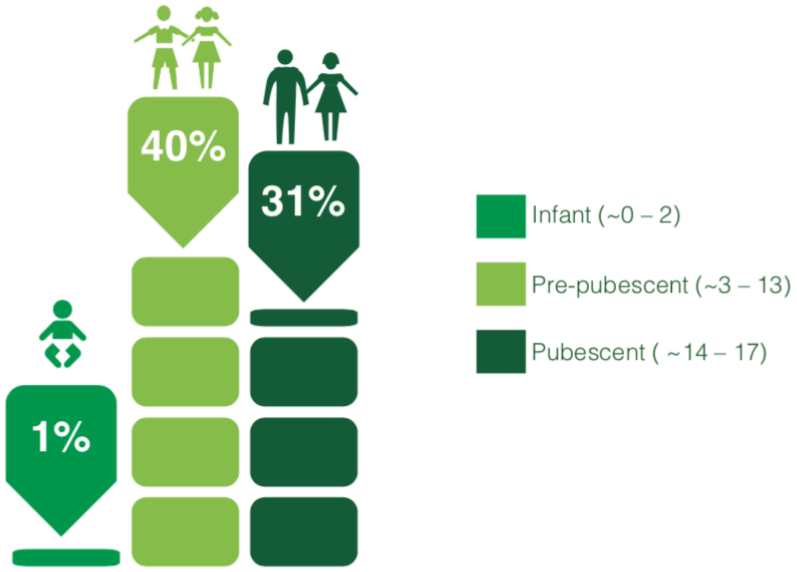
Fonte: http://www.inhope.org/Libraries/2016/INHOPE_2016_Statistics.sflb.ashx

CSAM Characteristics

Based on the content reported through ICCAM in 2016, we can see that the majority of CSAM encountered by hotlines depicts children that are predominantly females in the pre-pubescent age range.

This is particularly worrying given the adjacent rise in digital crimes such as coercion and extortion, which are increasingly the result of self-generated sexual images. Children of younger ages can be more prone to manipulation and targeting by online offenders, and with more access to technology than ever before, this is an issue that requires both preventative awareness raising and legal diligence.

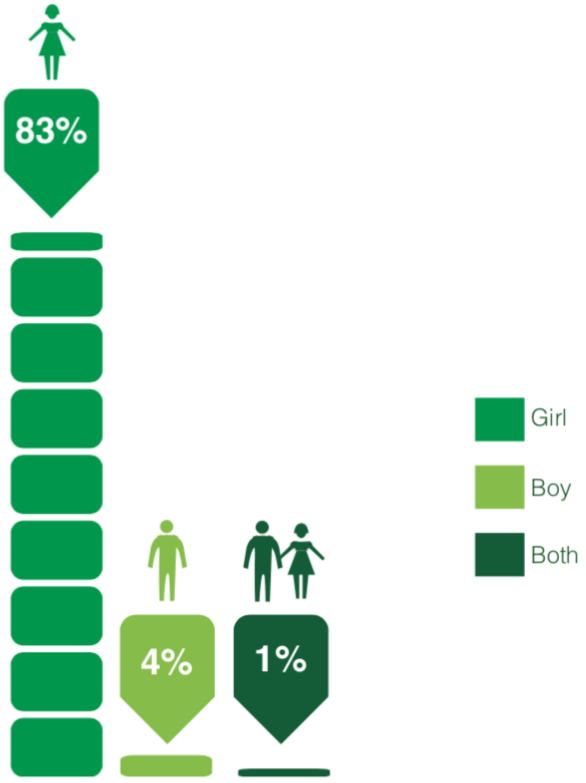
CSAM Characteristics - Age*



Picture: CSAM Characteristics: Age (n= 75,496)

* These figures reflect 72% of categorised data collected from reports through the ICCAM system.
* There are some national systems that have to be mapped onto ICCAM, which is a very new and innovative system. The 72% data points will become 100%.

CSAM Characteristics - Gender*



Picture: CSAM Characteristics: Gender (n= 43,902)

* These figures reflect 88% of determined data collected from reports through the ICCAM system.
* There are some national systems that have to be mapped onto ICCAM, which is a very new and innovative system. The 88% data points will become 100%.

Fonte: http://www.inhope.org/Libraries/2016/INHOPE_2016_Statistics.sflb.ashx

Hosting versus production, consumption and distribution

It is vital to recognise that hosting is only one part of the broader picture when it comes to the creation, distribution, and consumption of child sexual abuse material. While hosting reports can tell us where the highest concentration of servers containing CSAM are located, this should not be conflated with the production and consumption of CSAM, which can happen anywhere.

The sexual abuse and exploitation of children is a pervasive problem worldwide, and no country is immune. The absence of hosting information in a particular geographic region does not mean that abuse is not taking place, that digital abuse content is not being created, or that there are no victims in need. It is critical to understand that a lack (or lower amount) of reported data does not mean the problem does not exist.

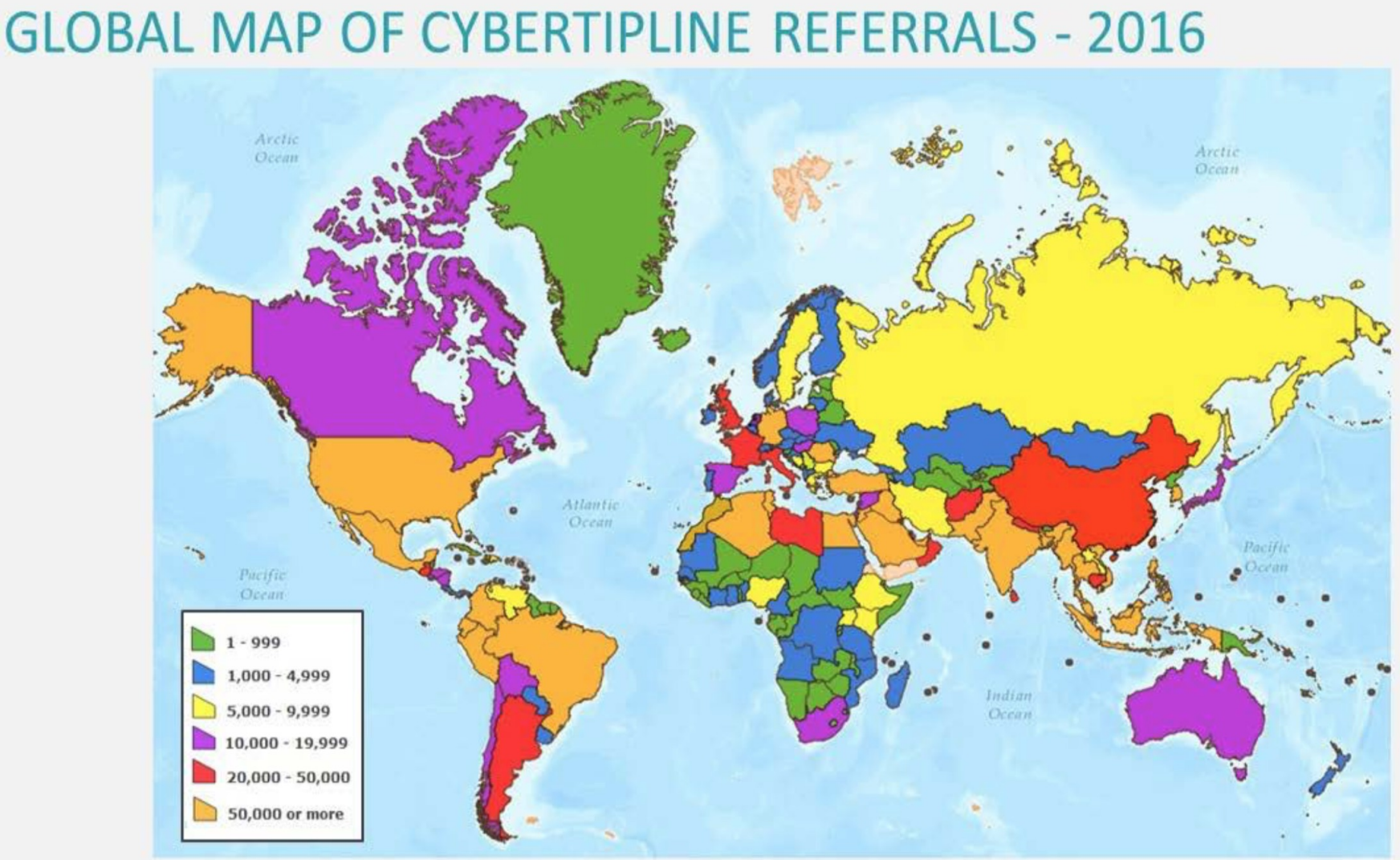
An example of this issue within INHOPE's own statistics is the representation of Africa, which may seem to indicate the absence of CSAM. To the contrary, as a region with only one current INHOPE hotline member, Africa highlights two important needs for improving the global status of CSAM:

1. A concerted effort to acknowledge the areas where gaps exist and create technical solutions accordingly. Enhanced insights and greater opportunities to protect children could come from establishing a developed reporting process. This is the case throughout Africa, as well as other regions of the world where better structure and support are often needed.

2. More research initiatives into the depth of child sexual abuse, particularly, but not limited to, developing regions. Evidence is needed to evaluate what drives the production, consumption, and dissemination of child sexual abuse material. In order to show a more accurate representation from every region and create a true global picture of the magnitude of CSAM, we must work toward a better understanding of each population.

http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2016.sflb.ashx

2016 Global Map of CyberTipline Reports (USA)



This map is not indicative of the level of child sexual abuse in a particular country.
This map depicts the volume of reports submitted predominantly by U.S.-based Electronic Service Providers to NCMEC's CyberTipline in accordance with 18 U.S.C. 2258A. Online companies report incidents of "apparent child pornography" and may include geographic indicators related to the incident. These geographical indicators may be affected by the use of proxies and anonymizers. This map is generated for informational purposes only.

http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2016.sflb.ashx

Internet Blocking

Crimes should be punished and not hidden

EUROPEAN
DIGITAL
RIGHTS

Fonte: https://edri.org/files/blocking_booklet.pdf

Internet Content Blocking Techniques					
	IP and Protocol-Based Blocking	**Deep Packet Inspection-Based Blocking**	**URL-Based Blocking**	**Platform-Based Blocking (especially search engines)**	**DNS-Based Blocking**
Overview	A device is inserted in the network that blocks based on IP address and/or application (e.g., VPN)	A device is inserted in the network that blocks based on keywords and/or other content (filename, for example)	A device is inserted in the network that intercepts web requests and looks up URLs against a block list	Working with application providers (such as search engines), content is modified according to local requirements	At the network or ISP level, DNS traffic is funneled to a modified DNS server that can block lookups of certain domain names
Is it effective?	Because IP addresses are easily changed and content easily moved, this technique works poorly. This only works well when the information publisher is not actively working to evade the block.	Where the blocked information is easily characterized, this is very effective. For general blocking (e.g., "block adult content") or in the face of encryption, the technique is very ineffective	This is a common technique that works well when blocking access to entire categories of information. New pages and smaller sites slip through easily, as do encrypted web servers.	Because there is no monopoly in search engines (for example) and consumer preferences are constantly changing, this type of blocking is largely cosmetic and works poorly.	DNS blocking is easily evaded both by content publishers and end users. DNS blocking is only effective when each name has a very small amount of content, and all that content should be blocked. Technical challenges, over-blocking, and ease of evasion make this an ineffective technique.
Who is affected?	Anyone who is "behind" the device is affected.	Anyone who is "behind" the device is affected.	Users "behind" the device, and for whom the device can intercept and evaluate web traffic.	Users of the search engine which has installed the block	Users of the modified DNS server. This can be enforced at the network or service provider level.
How specific is it?	Affects all content on a server, whether illegal or not. This works even when the data are encrypted.	Affects only content which matches blocking rules. Requires proxies to work with encrypted web pages.	Affects individual web pages and web elements. Requires proxies to work with encrypted web pages.	Affects individual web pages and elements. Usually done at the individual URL level.	Affects all content served by a domain name, whether illegal or not. Cannot be effectively used to distribute content.
What type of technique is this?	Blocks content	Blocks content	Blocks content	Discourages and frustrates access	Discourages and frustrates access
How much collateral damage is caused?	Any targeting of larger servers has a huge false positive rate, blocking both illegal and legal content.	Depending on the quality of the blocking rules, the false positive rate can range from very low to quite high. Writing good rules is difficult.	Most URL filtering is based on commercial services that categorize traffic. For mainstream blocks, this can be quite specific, but for special purpose blocks, the error rate is quite high.	The false positive rate is considered to be low, because each page block is requested individually. The problem of non-legitimate requests causes some inappropriate information to be blockage.	Any targeting of domain names used by larger servers has a huge false positive rate, blocking both illegal and legal content. Ineffective when CDNs are used (or causes an extremely high level of false positives).
What are common ways to evade it?	Publishers can change IP addresses, migrate content, or use Content Delivery Networks (CDNs) to evade. VPN users evade by hiding IP addresses.	Multiple layers of encryption effectively evade this type of blocking. When the filtering rules are poorly written, small changes in text can easily bypass blocks.	Multiple layers of encryption effectively evade this type of blocking. Use of non-standard application layer is often an effective evasion technique.	Users can choose alternative platforms, such as a different search engine, very easily.	Users can avoid using DNS lookups using local facilities, or can send their queries to an un-modified public server (typically though a VPN).
Are there side-effects or technical issues?	Maintaining long IP address lists is difficult and error-prone, and requires significant resources. Network devices doing this type of blocking are typically speedy, so performance issues are not common.	Content-aware filtering has significant performance costs and is not practical in many environments (without enormous resources). When proxies are used, security can be severely compromised.	URL filtering can cause performance problems, decreasing overall speed and reliability. When proxies are used, security can be severely compromised.	Many search engines report on "suppressed" information, which itself creates a trail to the content.	DNS security is compromised when a modified server is deployed.

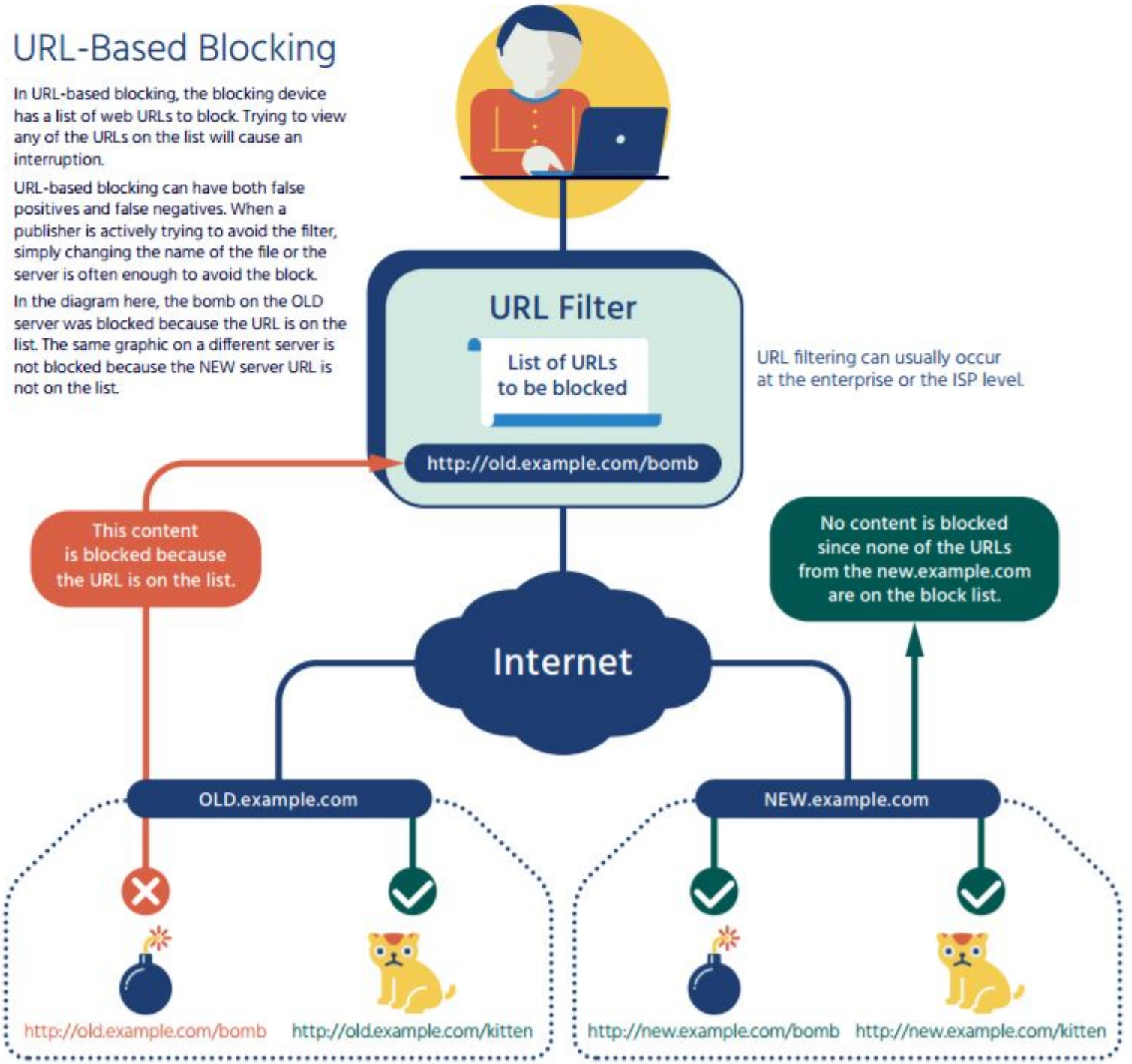
Fonte: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

URL-Based Blocking

In URL-based blocking, the blocking device has a list of web URLs to block. Trying to view any of the URLs on the list will cause an interruption.

URL-based blocking can have both false positives and false negatives. When a publisher is actively trying to avoid the filter, simply changing the name of the file or the server is often enough to avoid the block.

In the diagram here, the bomb on the OLD server was blocked because the URL is on the list. The same graphic on a different server is not blocked because the NEW server URL is not on the list.



IWF, Wikipedia and the “Wayback Machine”

Dr Richard Clayton
richard.clayton@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

UKNOF13, Sheffield
28th May 2009

Fonte: https://www.uknof.org.uk/uknof13/Clayton-IWF.pdf

Failures in a Hybrid Content Blocking System

Richard Clayton

University of Cambridge, Computer Laboratory, William Gates Building,
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom

richard.clayton@cl.cam.ac.uk

Abstract. Three main methods of content blocking are used on the Internet: blocking routes to particular IP addresses, blocking specific URLs in a proxy cache or firewall, and providing invalid data for DNS lookups. The mechanisms have different accuracy/cost trade-offs. This paper examines a hybrid, two-stage system that redirects traffic that might need to be blocked to a proxy cache, which then takes the final decision. This promises an accurate system at a relatively low cost. A British ISP has deployed such a system to prevent access to child pornography. However, circumvention techniques can now be employed at both system stages to reduce effectiveness; there are risks from relying on DNS data supplied by the blocked sites; and unhappily, the system can be used as an *oracle* to determine what is being blocked. Experimental results show that it is straightforward to use the system to compile a list of illegal websites.

Fonte: https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

British censor reverses Wikipedia ban

Unprecedented decision sees temporary online ban lifted on controversial 32-year-old album cover

Britain's internet censor has backtracked on its decision to ban a Wikipedia page for containing a "potentially illegal" image of a naked child.

Over the weekend it emerged that the Internet Watch Foundation, which operates a blacklist to screen out images of child abuse that is used by the majority of British internet providers, had banned the image of a 32-year-old album cover by German rock group The Scorpions.

The decision resulted in a technical glitch which prevented thousands of British web surfers from editing any pages on Wikipedia, as well as confusion over why the image was deemed "potentially illegal" - particularly since the album itself has been on sale in high street shops for more than 30 years.

But after conducting a review of the decision, and amid protests from the Wikimedia organisation on Monday, the IWF today said that it would make the unprecedented decision to reverse its position and remove the image from its

Wikipedia falls foul of British censors

Wikipedia page blacklisted over 'potentially illegal' album cover from 1976

Internet Content Blocking Techniques					
	IP and Protocol-Based Blocking	**Deep Packet Inspection-Based Blocking**	**URL-Based Blocking**	**Platform-Based Blocking (especially search engines)**	**DNS-Based Blocking**
Overview	A device is inserted in the network that blocks based on IP address and/or application (e.g., VPN)	A device is inserted in the network that blocks based on keywords and/or other content (filename, for example)	A device is inserted in the network that intercepts web requests and looks up URLs against a block list	Working with application providers (such as search engines), content is modified according to local requirements	At the network or ISP level, DNS traffic is funneled to a modified DNS server that can block lookups of certain domain names
Is it effective?	Because IP addresses are easily changed and content easily moved, **this technique works poorly.** This only works well when the information publisher is not actively working to evade the block.	Where the blocked information is easily characterized, this is very effective. For general blocking (e.g., "block adult content") or in the face of encryption, **the technique is very ineffective**	This is a common technique that **works well when blocking access to entire categories** of information. New pages and smaller sites slip through easily, as do encrypted web servers.	Because there is no monopoly in search engines (for example) and consumer preferences are constantly changing, **this type of blocking is largely cosmetic and works poorly.**	DNS blocking is easily evaded both by content publishers and end users. DNS blocking is only effective when each name has a very small amount of content, and all that content should be blocked. **Technical challenges, over-blocking, and ease of evasion make this an ineffective technique.**
Who is affected?	Anyone who is "behind" the device is affected.	Anyone who is "behind" the device is affected.	Users "behind" the device, and for whom the device can intercept and evaluate web traffic.	Users of the search engine which has installed the block	Users of the modified DNS server. This can be enforced at the network or service provider level.
How specific is it?	**Affects all content on a server, whether illegal or not.** This works even when the data are encrypted.	**Affects only content which matches blocking rules.** Requires proxies to work with encrypted web pages.	**Affects individual web pages and web elements.** Requires proxies to work with encrypted web pages.	**Affects individual web pages and elements.** Usually done at the individual URL level.	**Affects all content served by a domain name, whether illegal or not.** Cannot be effectively used to distribute content.
What type of technique is this?	Blocks content	Blocks content	Blocks content	Discourages and frustrates access	Discourages and frustrates access
How much collateral damage is caused?	Any targeting of larger servers has a huge false positive rate, blocking both illegal and legal content.	Depending on the quality of the blocking rules, the false positive rate can range from very low to quite high. Writing good rules is difficult.	Most URL filtering is based on commercial services that categorize traffic. For mainstream blocks, this can be quite specific, but for special purpose blocks, the error rate is quite high.	The false positive rate is considered to be low, because each page block is requested individually. The problem of non-legitimate requests causes some inappropriate information to be blockage.	Any targeting of domain names used by larger servers has a huge false positive rate, blocking both illegal and legal content. Ineffective when CDNs are used (or causes an extremely high level of false positives).
What are common ways to evade it?	Publishers can change IP addresses, migrate content, or use Content Delivery Networks (CDNs) to evade. VPN users evade by hiding IP addresses.	Multiple layers of encryption effectively evade this type of blocking. When the filtering rules are poorly written, small changes in text can easily bypass blocks.	Multiple layers of encryption effectively evade this type of blocking. Use of non-standard application layer is often an effective evasion technique.	Users can choose alternative platforms, such as a different search engine, very easily.	Users can avoid using DNS lookups using local facilities, or can send their queries to an un-modified public server (typically though a VPN).
Are there side-effects or technical issues?	Maintaining long IP address lists is difficult and error-prone, and requires significant resources. Network devices doing this type of blocking are typically speedy, so performance issues are not common.	Content-aware filtering has significant performance costs and is not practical in many environments (without enormous resources). When proxies are used, security can be severely compromised.	URL filtering can cause performance problems, decreasing overall speed and reliability. When proxies are used, security can be severely compromised.	Many search engines report on "suppressed" information, which itself creates a trail to the content.	DNS security is compromised when a modified server is deployed.

Fonte: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

Muito obrigado!

thiagotavares@safernet.org.br