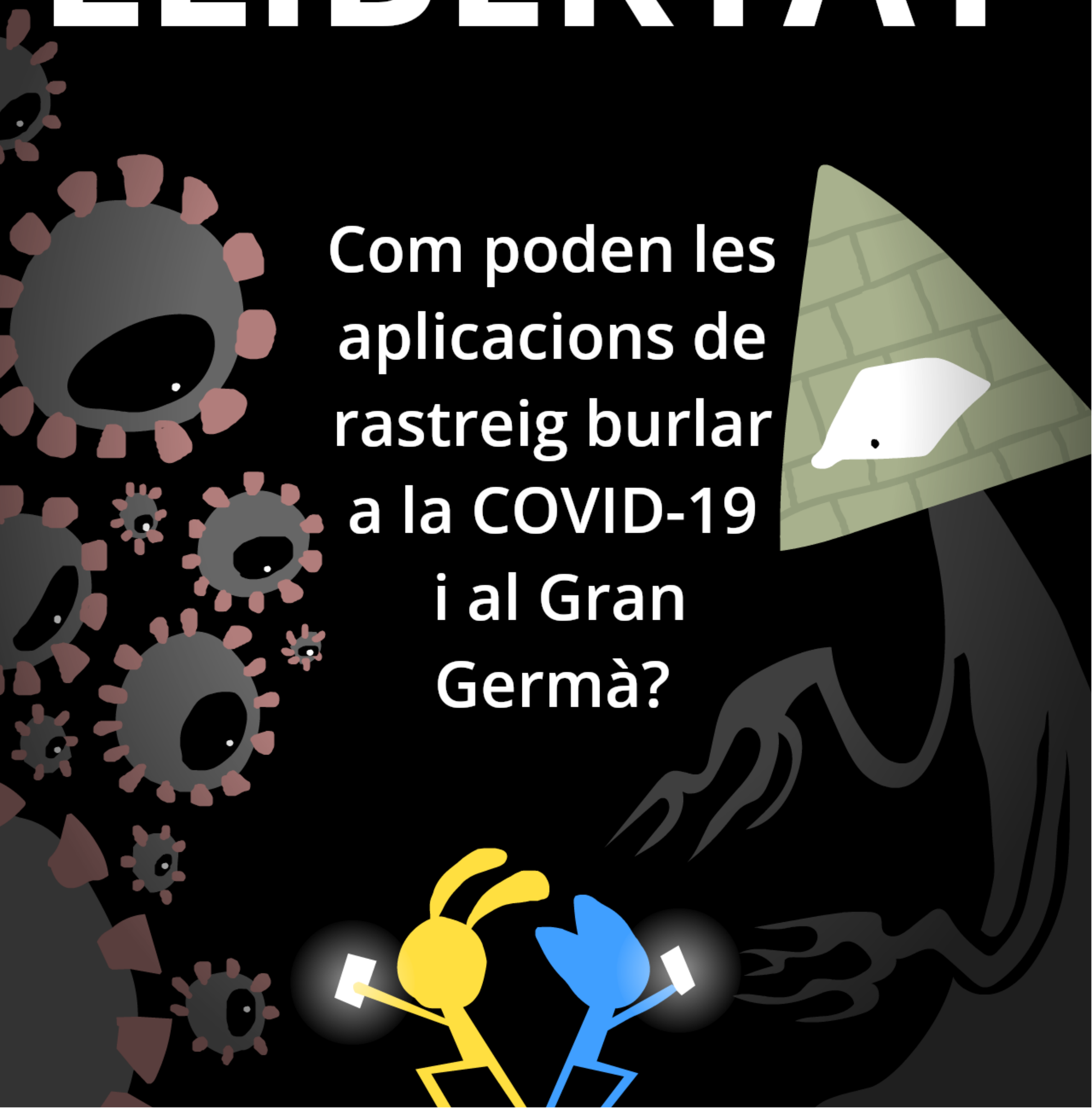
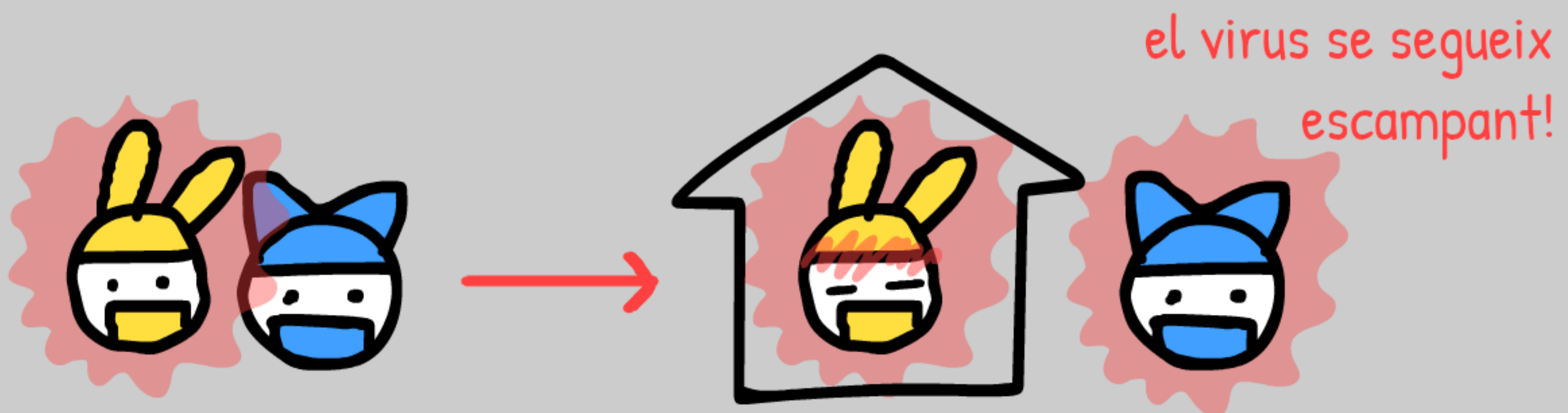


PROTEGINT VIDES I LA LLIBERTAT

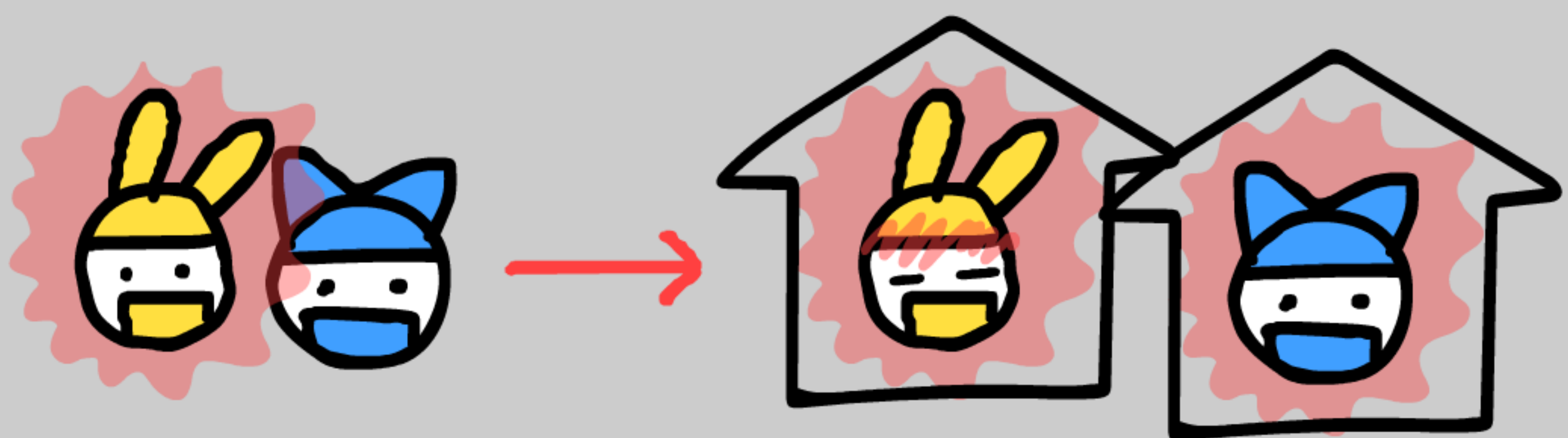
Com poden les
aplicacions de
rastreig burlar
a la COVID-19
i al Gran
Germà?



Un problema de la COVID-19:
Ets contagiós ~2 dies *abans* de
saber que has estat infectat.



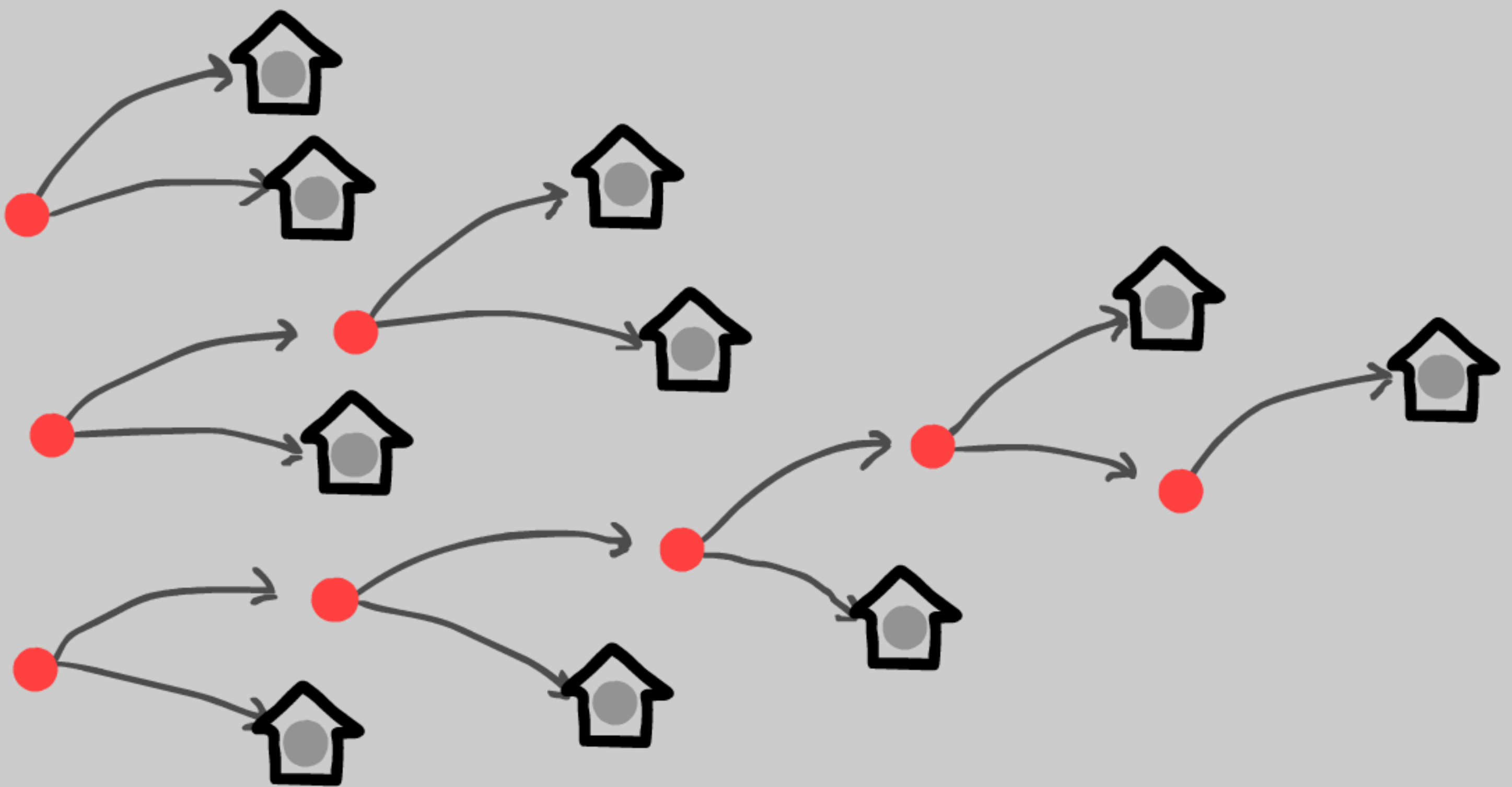
Es triga ~3 dies en *tornar-se* contagiós,
llavors si posem en quarantena a qui hagi
estat en contacte amb tu *tan bon punt*
sàpigues que has estat infectat...



Podem aturar la seva propagació
avançant-nos a ella!

*I què passa amb els casos *asimptomàtics*? Sembla ser que no tenen un gran impacte en la propagació de la COVID-19! (veure fonts al final)

Això es coneix com a "rastreig de contactes". Ha estat una de les claus de l'èxit en la contenció del virus per part de Corea del Sud i Taiwan i ha de ser-ho per a nosaltres també.



Ni tan sols necessitariem trobar a tots els contactes! Seria suficient amb un ~60% d'ells...

*Només un ~60%? De nou, veure les fonts al final.

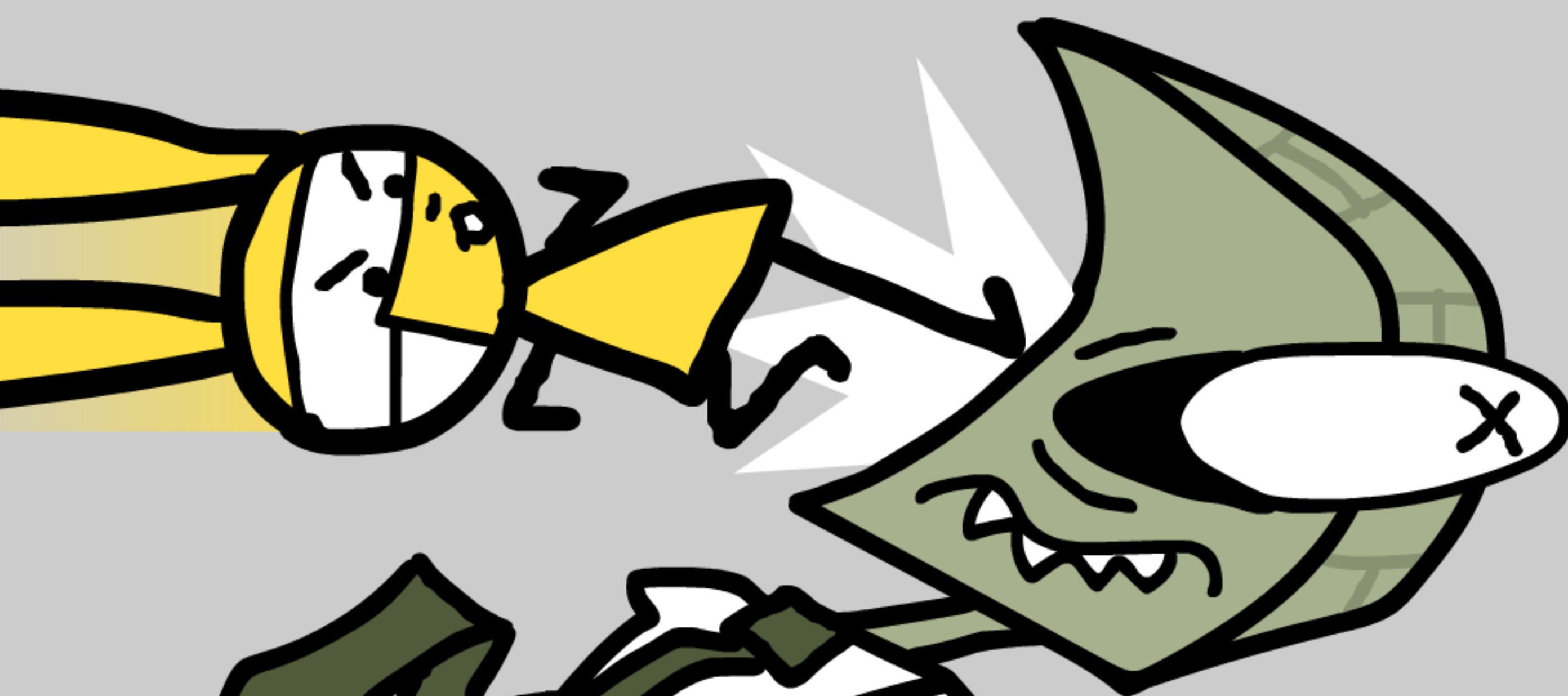
...però *hem de* trobar-los ràpidament.
Rastrear els contactes de forma
tradicional mitjançant entrevistes és
massa lent.

I és per això que
necessitem
aplicacions de
rastreig.

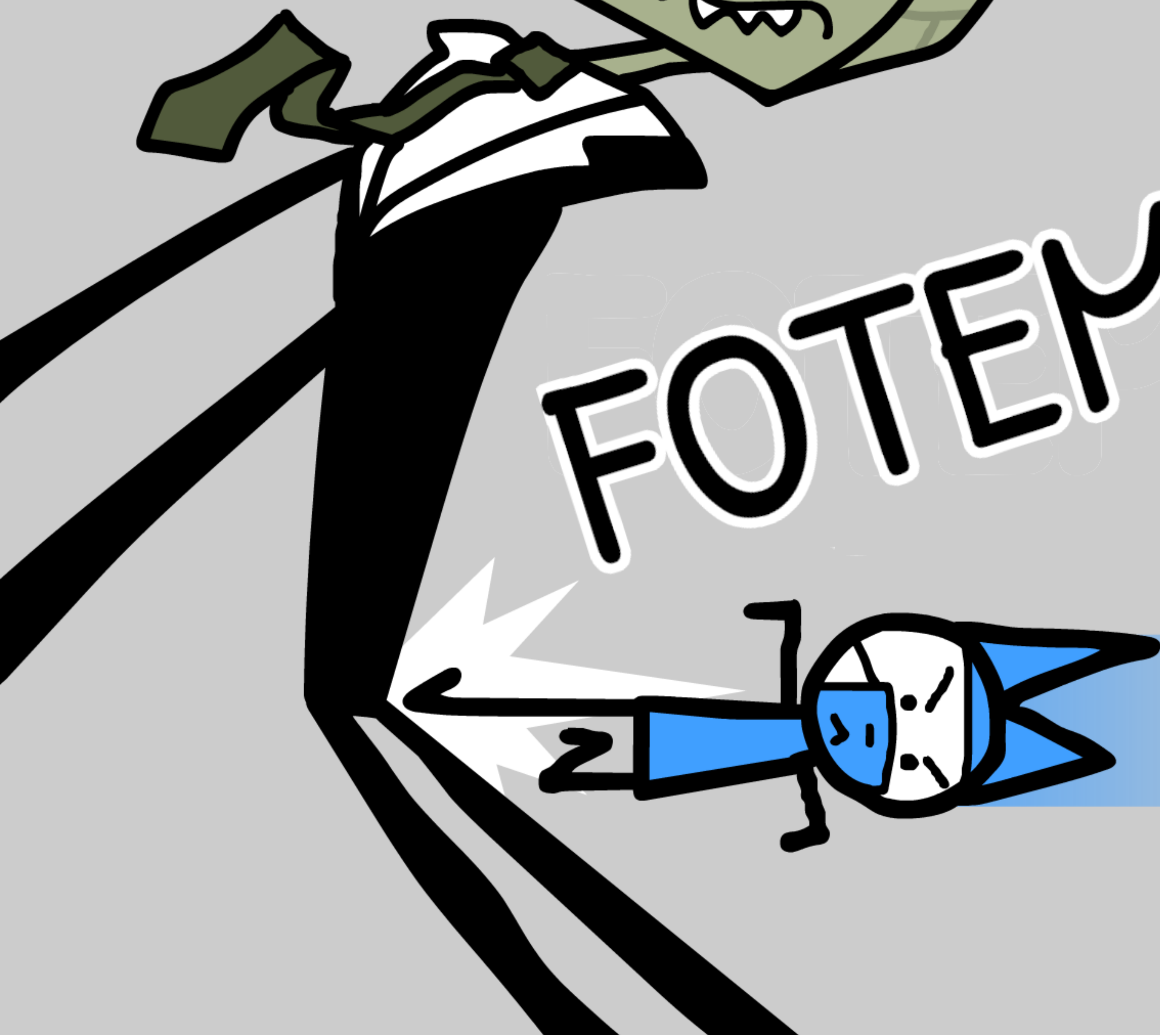
Hem de sacrificar la
nostra privacitat
a canvi de la
salut?



NO



FOTEM!

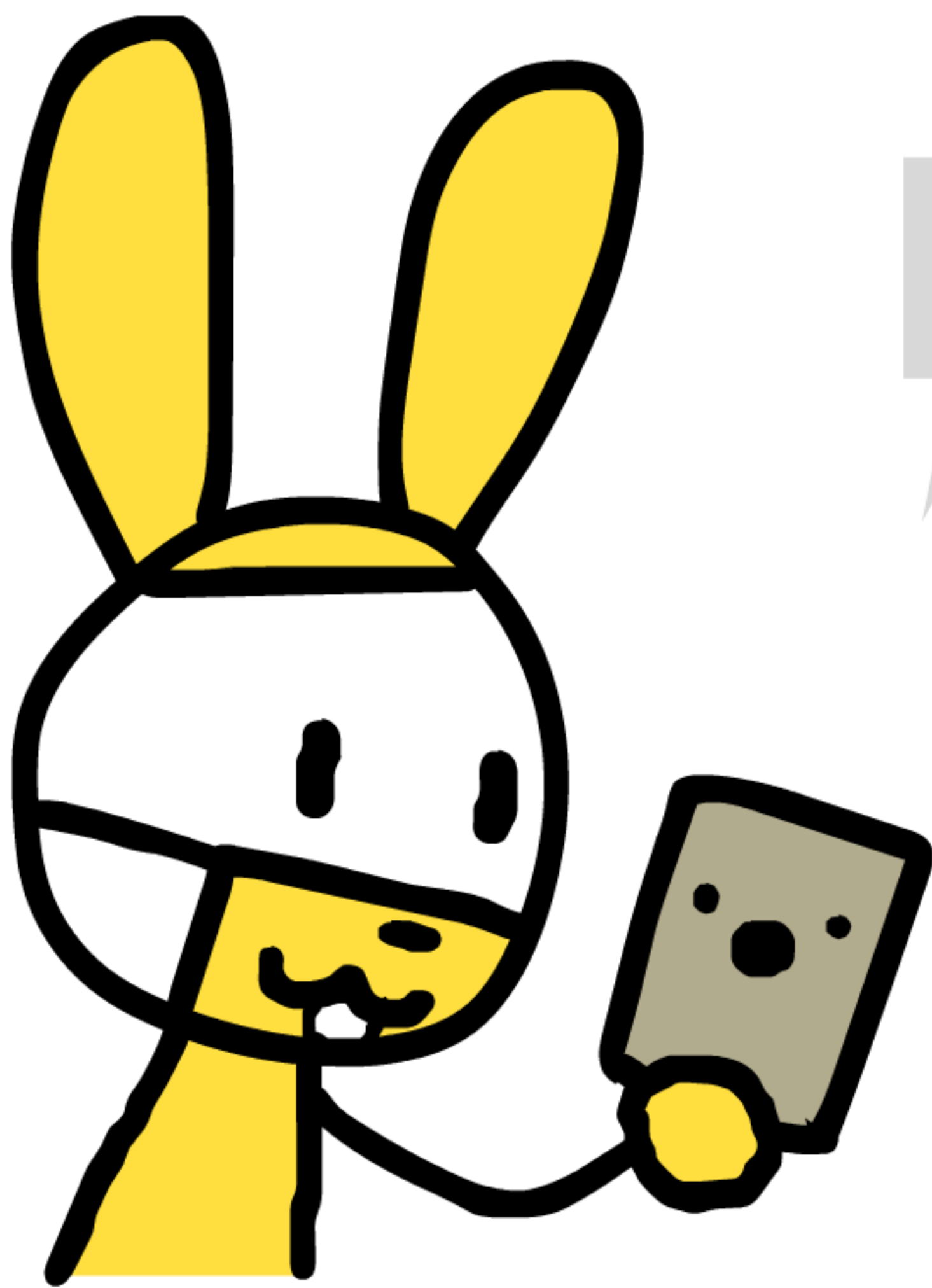


És del tot possible protegir la
vida de les persones I TAMBÉ
la seva llibertat amb un procés
ben simple!

Anem a veure com
funciona amb l'ajuda de
l'Alice i en Bob...



L'Alice s'instal·la una aplicació de rastreig! (de codi obert, de forma que qualsevol pugui verificar que realment fa el que hauria...)



51Pomk

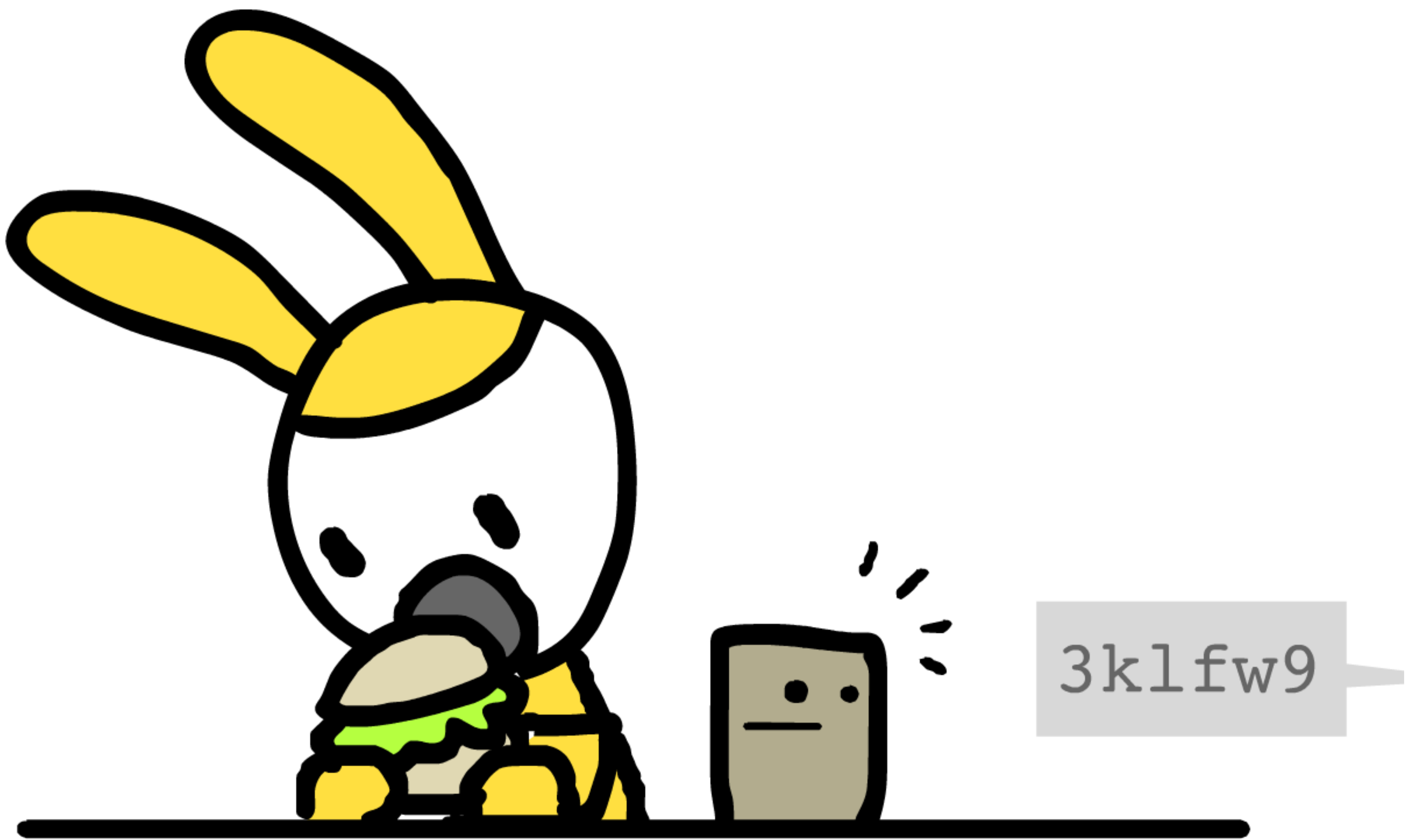
8jUILL4

11wda6

Cada 5 minuts, el seu mòbil envia un codi aleatori únic a tots els dispositius propers a través de Bluetooth.

*Els 5 minuts són només un exemple. Tècnicament, cada codi és en realitat "pseudo-aleatori" ja que no han estat generats de forma quàntica... pero NO importa.

Donat que aquests missatges són aleatoris i no usen GPS, no contenen CAP DADA sobre la identitat de l'Alice, la seva localització o qualsevol altre cosa.



Mentre el seu mòbil envia aquests missatges aleatoris, aquest també està *escoltant* els missatges d'altres mòbils propers.

Per exemple, el d'en Bob.

En Bob també disposa d'una aplicació de rastreig que fa èmfasi en la seva privacitat, i és compatible amb la de l'Alice (o és la mateixa).



Si l'Alice i en Bob es troben a prop durant 5 o més minuts, els seus mòbils aniran intercanviant codis aleatoris.

Tots dos mòbils recorden tots els missatges que han enviat i escoltat en els darrers 14 dies.



Recordem: donat que els missatges aleatoris NO CONTENEN CAP DADA, la privacitat de l'Alice es troba protegida envers en Bob, i viceversa.

*Els 14 dies són només un exemple. Els epidemiòlegs podrien descobrir que el "període d'infecció" és en realitat més curt o més llarg.

En el dia següent, l'Alice comença a tenir tos seca i febre.

L'Alice es fa una prova.



L'Alice té la COVID-19.
No és un bon dia per a l'Alice.

El seu patiment, però, no serà en va! L'Alice envia la seva llista de missatges "ALLÒ QUE HE DIT" a la base de dades d'un hospital, usant un mot clau d'un sol ús proporcionada pel seu metge.

(El mot clau és per evitar *spam*)

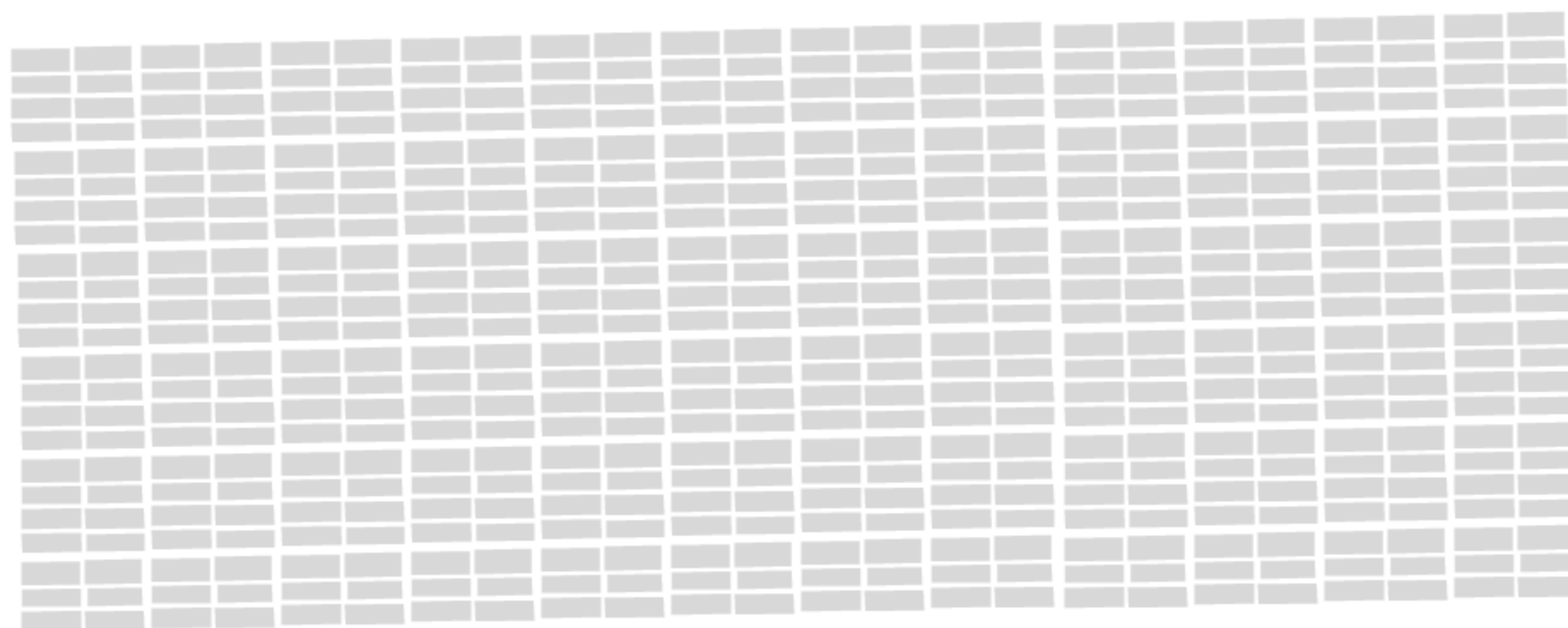


L'Alice pot ocultar missatges de moments que prefereixi mantenir en privat, com ara les nits a casa.

La base de dades emmagatzema els missatges de l'Alice:



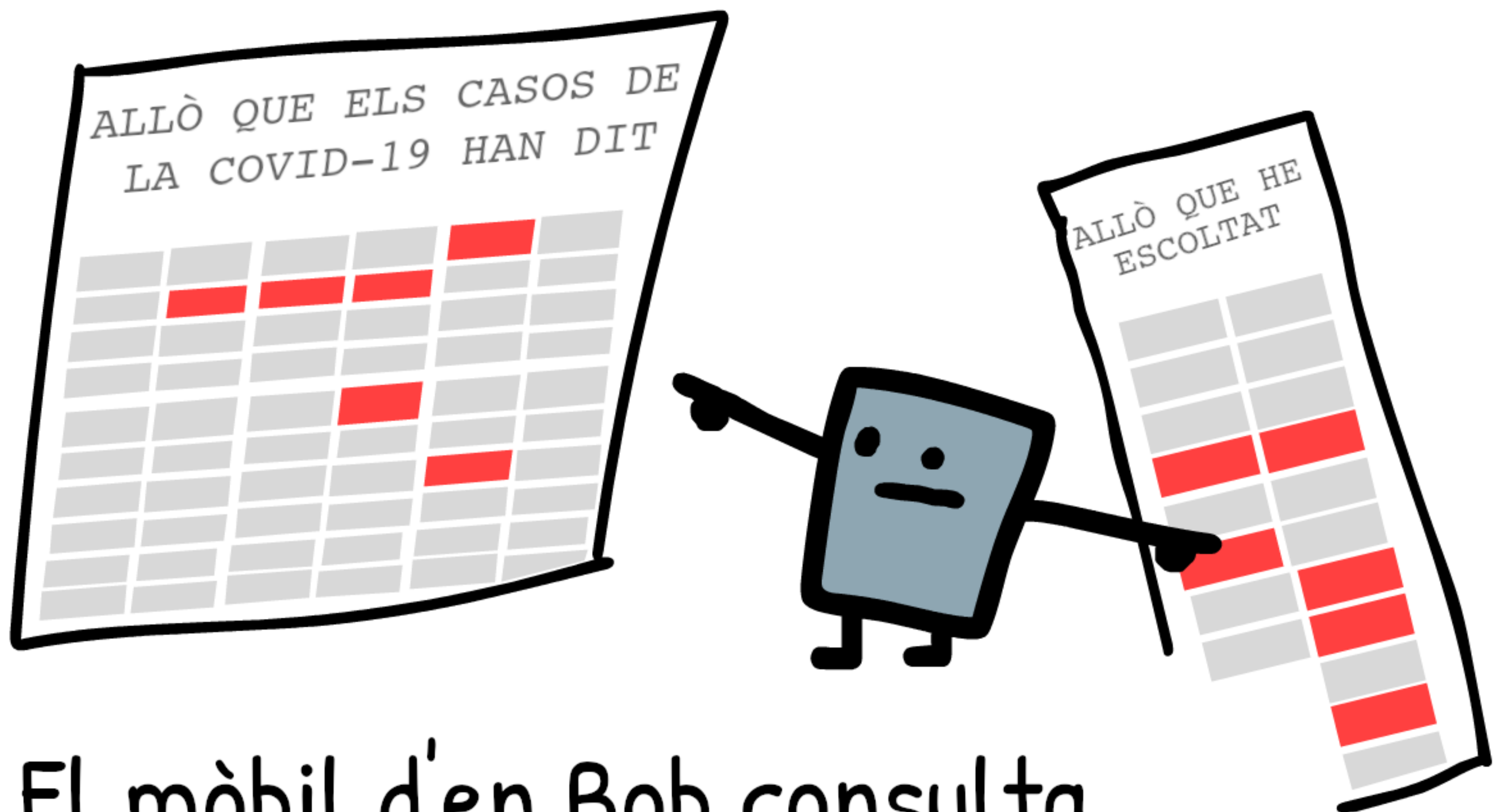
ALLÒ QUE ELS CASOS DE
LA COVID-19 HAN DIT



Recordem: aquests missatges aleatoris no proporcionen a l'hospital CAP DADA sobre on era l'Alice, amb qui es trobava, què estava fent... ni tan sols amb quanta gent estava! És del tot irrellevant per a l'hospital...

*Hospitals de diferents països podrien intercanviar aquests missatges, però en no contenir cap informació, no es perd la privacitat.

... però no per a en Bob!

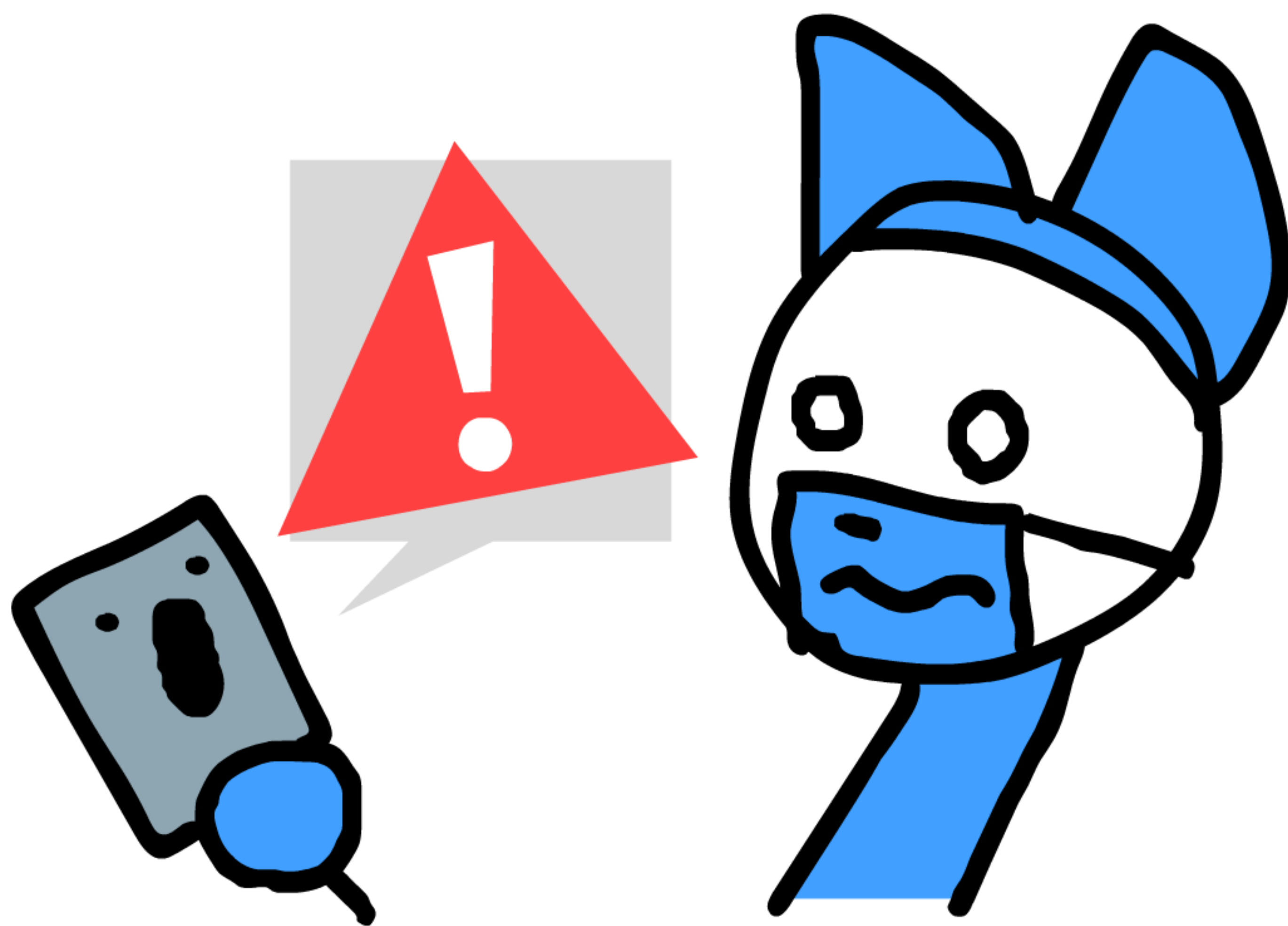


El mòbil d'en Bob consulta regularment la llista de missatges aleatoris de l'hospital per tal de comprovar si cap dels que ha "escoltat" en els darrers 14 dies es troben en ella.

(Aquests missatges no li ofereixen a en Bob CAP ALTRA DADA PERSONAL).

*El protocol DP-3T real és fins i tot MÉS segur. Usa un "filtre de cucut" de forma que els mòbils coneixen ÚNICAMENT els missatges que han escoltat, sense revelar LA RESTA de missatges.

Posem que ha escoltat 6 o més missatges (6 x 5 min indica una exposició de mitja hora), llavors el mòbil avisa en Bob per a que es posi en quarantena.



I així és com en Bob talla la cadena de transmissió, estant un pas per endavant del virus!

*Aquests números són, un cop més, exemples.

I això és tot!

Així és com el rastreig digital de contactes pot prevenir la propagació de la COVID-19 de forma proactiva *garantint també* els nostres drets.



Moltes gràcies a
l'Alice i en Bob!
Cuideu-vos!

FONTS

Aquest còmic és un esbós del protocol **DP-3T** amb data de 9 d'abril de 2020. El protocol de veritat és molt més complex i encara més segur! Llegiu-ne l'article:

github.com/DP-3T/documents

Existeix un altre sistema similar de protecció de privacitat anomenat **Protocol TCN**. Us en podeu informar aquí: github.com/TCNCoalition/TCN

Per acabar, aquí teniu l'estudi de la Universitat d'Oxford que mostra com les aplicacions de rastreig de contactes podrien contenir la COVID-19 sense confinaments prolongats!

Ferretti & Wymant et al. "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing." *Science* (2020).

Aquest còmic és de **DOMINI PÚBLIC**

Això significa que *ja* disposes de permís per a redistribuir-lo en el teu web. Ens encantaria que l'incloguessis en la teva pròpia aplicació de rastreig (sempre i quan aquesta compleixi exactament amb el protocol de protecció de privacitat descrit).

També tens permís per a traduir aquest còmic! Les fonts usades són "Patrick Hand" i "Open Sans".

Traduït al català per Xavi R. Pinteño.



per **Nicky Case**

ncase.me + patreon.com/ncase

amb la inestimable ajuda de la
Prof. **Carmela Troncoso** (seguretat)
i el Prof. **Marcel Salathé** (epidemiologia)