

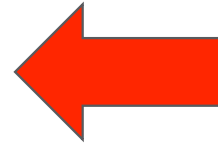
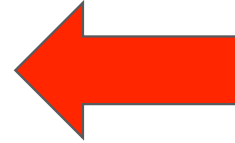
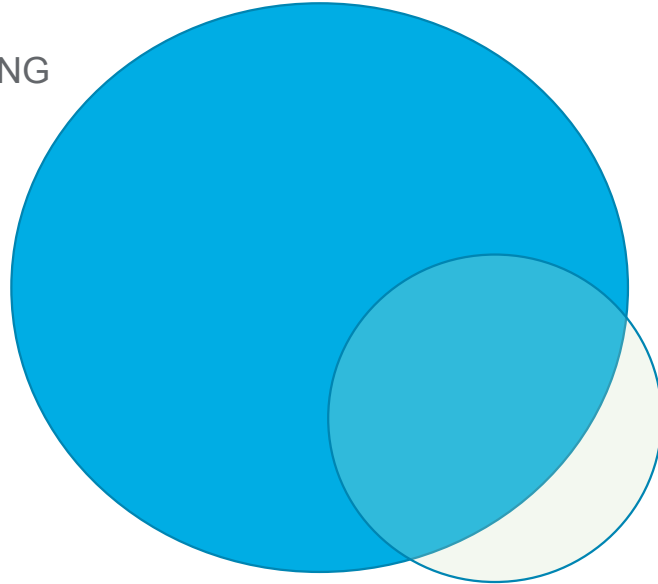
20 NOVEMBER 2017

# PRIVACY EN INFORMATIEVEILIGHEID

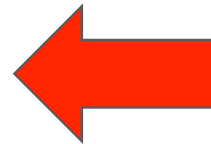
## ZOEKEN NAAR EEN NIEUW EVENWICHT

# PRIVACY ONDERDEEL VAN INFORMATIEBEVEILIGING?

INFORMATIEBEVEILIGING



PRIVACY



## Gepubliceerd in het Staatsblad op 17 augustus 2017

- Inlichtingendiensten krijgen vergaande bevoegdheden om in bulk persoonsgegevens te onderscheppen, te analyseren en door te geven aan andere diensten.
- Inlichtingendiensten mogen apparatuur van targets hacken (gebruiken, malware plaatsen, etc.).
- Inlichtingendiensten krijgen toegang tot data over de kabel.
- Diensten mogen via derden-netwerk toegang verkrijgen.

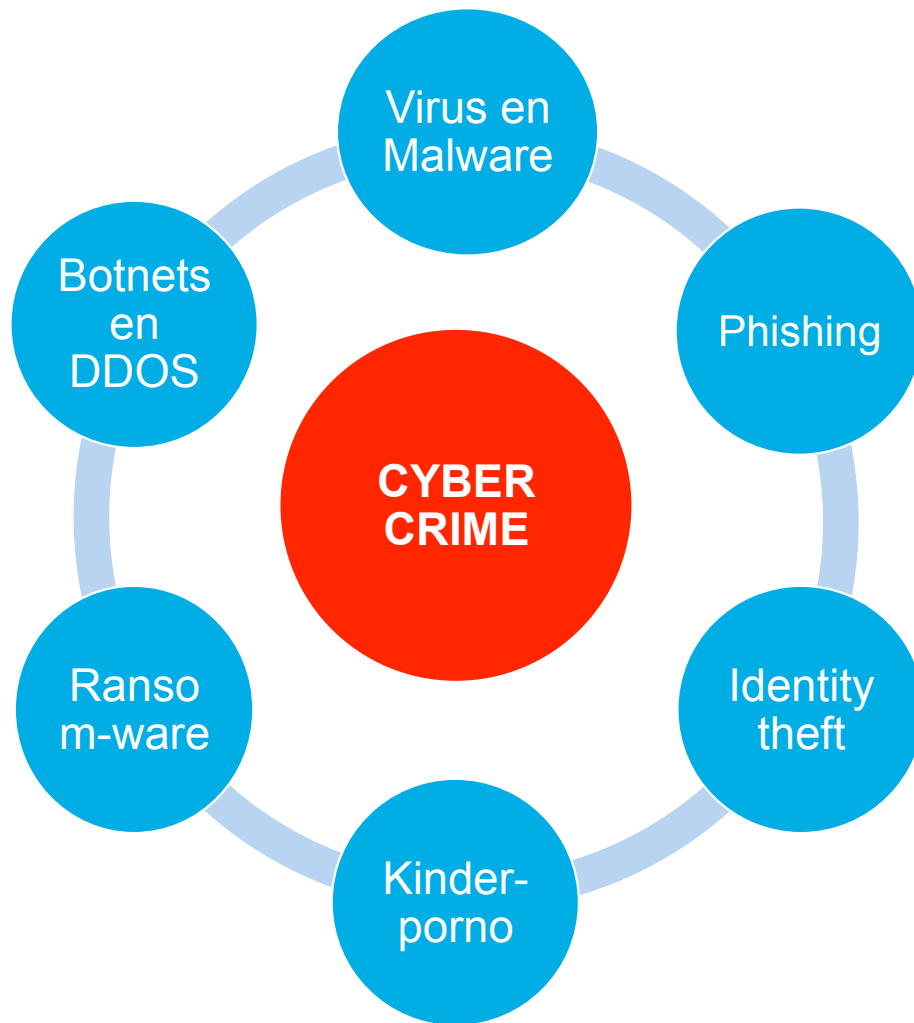
- Wetsvoorstel aangenomen door 2e kamer op 20-12-2016.
- Eerste kamer heeft op 5-9-2017 nader voorlopig verslag uitgebracht.
- Politie en Justitie mogen heimelijk en op afstand onderzoek doen in computers.
- Verderegaande bevoegdheden
  - opsporingsambtenaren
    - Destructie van gegevens
    - Kopiëren van data
    - Aftappen
    - Observeren

# ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

- Verordening van 25 mei 2016
- Ingangsdatum 25 mei 2018

Voor de gehele EU (28 lidstaten een uniforme regelgeving rondom de privacyrechten van EU-ingezetenen.





# FUNDAMETEELE RECHTEN VAN DE MENS



RECHT OP VEILIGHEID



EVRM



RECHT OP PRIVACY

# VEILIGHEID EEN INBREUK OP HET RECHT OP PRIVACY?

- Noodzakelijk?
  - Proportioneel (niet meer dan nodig).
  - Subsidiariteit (kan het met minder).
- Vrijheid van meningsuiting?
- Effectief?
- Waarborgen tegen willekeur?
  - Vernietiging van niet relevante gegevens.
  - Bewaren van nog niet onderzochte data.
  - Profielen, algoritmen en methoden niet transparant.
- Toezicht? TIB-commissie heeft geen onderzoeksbevoegdheid.



# GEGEENSVERWERKING EEN INBREUK OP PRIVACY?

- De AVG heeft geen meldplicht voor verwerking van persoonsgegevens, zoals de WBP.
- Verwerkingen van persoonsgegevens met een hoog risico voor rechten van betrokkenen: DPIA verplicht.
- Indien uit DPIA blijkt dat de organisatie geen risico beperkende maatregelen treft: verwerking vooraf laten toetsen door AP.



## PERSONEELSDOSSIER IN STRIJD MET PRIVACY?

- Voor sollicitaties mag geen kopie ID-bewijs gemaakt.
- Gegevens niet langer bewaren dan nodig.
- Verboden om aard en oorzaak van ziekten te registreren.
- CV's van sollicitanten mogen alleen in de daarvoor bestemde databases worden opgeslagen, niet in (semi-)privé omgevingen zoals b.v. e-mail.

# SCREENING EEN INBREUK OP PRIVACY?

- In bepaalde gevallen is screening van sollicitanten of werknemers toegestaan. (kinderopvang).
- Toestemming betrokkene is *geen wettelijke grondslag* (er is geen sprake van vrije toestemming).
- Mag alleen op onderdelen die risico's verminderen.
- Proportioneel met risico van de functie (Geen sociaal media profiel toevoegen).

# CAMERATOEZICHT EEN INBREUK OP PRIVACY?

- In bepaalde gevallen is cameratoezicht toegestaan (gerechtvaardigd belang: diefstal, vandalisme).
- Audio is niet toegestaan (geen doelbinding).
- Mag alleen op onderdelen die risico's verminderen.
- Proportioneel met risico van de functie
- Subsidiariteit: kan het ook minder ingrijpend?
- Alleen als onderdeel van een totaalpakket
- Bewaartermijn van beelden is meestal 4 weken.

# PASSENGER NAME RECORDS (PNR) EN PRIVACY

Boekingsgegevens die reisorganisaties en vervoersmaatschappijen registreren (reisgezelschap, reisvoorkeuren, speciale verzoeken, gegevens over de betaalwijze, bagage-informatie en zitplaatsnummer).

- Opsporingsdiensten willen graag toegang t.b.v. profiling van criminelen.
- PNR data bevatten ook bijzondere persoonsgegevens → verwijderen.
- Doorgifte buiten EU verboden, m.u.v. verdaglanden (USA, Canada, Australië)/
- Bewaartermijn, doorgifte en lokaal toezicht.

# Het recht op privacy is niet eenvoudig geïmplementeerd. We moeten op zoek naar een nieuwe balans.

- Staat soms op gespannen voet met recht op veiligheid
- De AVG is principle based. Het is aan de verantwoordelijke om zijn keuze te onderbouwen
- Overheden hebben soms een andere opvatting over privacy
- Criminelen houden zich niet aan privacyregels
- Opsporingsdiensten hebben behoefte aan ruime privacyregels



**M. (Rien) Hommes RE RA**  
Head of Risk Management / partner

T +31 (0)45 405 55 55

E [rhommes@rsm-nl.nl](mailto:rhommes@rsm-nl.nl)