alia
connecting security interests

Welkom op onze Security Day 2024

Bienvenue à notre Security Day 2024

Nelectra
Federatie voor de elektrosector

ELOYA
union des électriciens
unie van elektriciens

Techlink
Linking technicians

FEE

ANPI

NEW SECURITY MAGAZINE

Programma

- WOORD VAN DE VOORZITTER
- DOLERO
- INCERT
- ANPI
- EURALARM
- PAUZE
- FOD TEAM INSPECTIES
- MARVA
- OZOOS
- UGENT
- MINISTRY OF PRIVACY

Programme

- MOT DU PRESIDENT
- DOLERO
- INCERT
- ANPI
- EURALARM
- PAUZE
- SPF TEAM INSPECTIONS
- MARVA
- OZOOS
- UGAND
- MINISTRY OF PRIVACY

alia
connecting security interests

Johan Chenot

Woord van de voorzitter
Mot du président

Change is Coming

alia
connecting security interests

Change is Coming

Work Life Balance

alia
connecting security interests

Change is Coming

Working together

alia
connecting security interests

Change is Coming

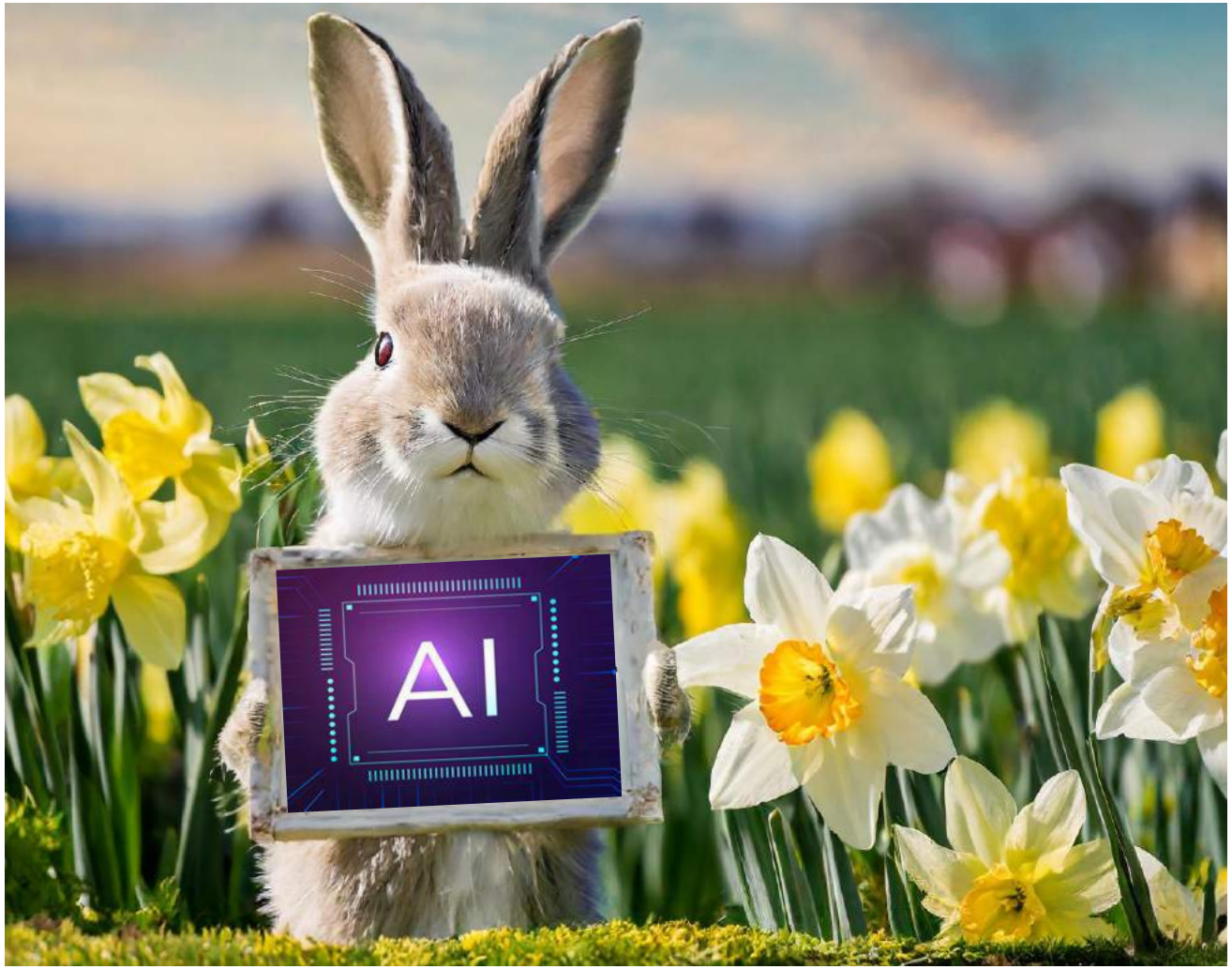
ELOYA union des électriciens unie van elektriciens — www.eloya.be — e-mail: info@eloya.be

Nelectra Federatie voor de elektrosector — www.nelectra.be — e-mail: info@nelectra.be

Techlink Linking technicians — www.techlink.be — e-mail: info@techlink.be

alia connecting security interests

Change is Coming



alia
connecting security interests

Change is Coming

Training

alia
connecting security interests

Change is Coming

Installer

connecting security interests

Change is Coming

Risk Analyse

alia
connecting security interests

Change is Coming

Quality Label

alia
connecting security interests

Change is Coming

alia
connecting security interests

Donald Leeuws

De do's en de don't bij de digitalisering van jouw onderneming

Ce qu'il faut faire et ne pas faire pour numériser votre entreprise

GOEDE MORGEN / BONJOUR

DOLERO

alia
connecting security interests

Behoefte / Besoin

- Gesprekken / Entretiens
- Reclame / Publicité
- Gebrek aan efficiëntie / Manque d’éfficacité
- Vraag van de markt / Demande du marché
- Wetgeving / Législation

Behoefte / Besoin

- Planning / Planification
- Contractbeheer / Gestion de contrats
- Servicebons / Documents de service
- Aankopen materialen / Achats des matériaux
- Voorraad / Inventaire
- Getekende bonnen & archivering / Documents signés & Archivage
- Facturatie / Facturation
- Boekhouding / Comptabilité
- Geld ontvangen / Réception d’argent

DOLERO

alia
connecting security interests

Behoefte / Besoin

- Voorraad / Inventaire
  - Goederenontvangst / Réception des biens
  - Verzending / Envoi
  - Min / Max

DOLERO

alia
connecting security interests

AS IS Situatie / Situation AS IS

Beschrijving van alle bedrijfsprocessen / Description de tous les processus d'affaires

- Gedetailleerd / Détaillée
- Per process / Par processus
- Link naar andere processen / Liaison vers autres processus
- Bij voorkeur gemodelleerd / De préférence de manière modellé (BPM)
- ≠ Manual van de bestaande software / ≠ Manuelle du logiciel existant

AS IS Situatie / Situation AS IS

Beschrijving van alle bedrijfsprocessen / Description de tous les processus d'affaires

- Uzelf / Vous même
- Interne IT afdeling / Département interne ICT
- Medewerkers per process / Collaborateurs par Processus
- Softwareleverancier / Fournisseur de logiciels – RFP ??
- (Ondersteund door) onafhankelijke expert / (Supporté par) expert indépendant.

ATIJD COMMUNICATIE MET GANSE ORGANISATIE / TOUJOURS COMMUNICATION AVEC TOUTE L'ORGANISATION

TO BE Situatie / Situation TO BE

Lastenboek / Cahier des charges

- Alle processen uit AS IS / Tous les processus de AS IS
- Definitie Scope / Définition du Scope (Processen / Processus)
- Impact op “Out of Scope” / Impact sur “Out of Scope”

TO BE Situatie / Situation TO BE

Lastenboek / Cahier des charges

- Uzelf / Vous même
- Interne IT afdeling / Département interne ICT
- Medewerkers per process / Collaborateurs par Processus
- Softwareleverancier / Fournisseur de logiciels – RFP ??
- (Ondersteund door) onafhankelijke expert / (Supporté par) expert indépendant.

ATIJD COMMUNICATIE MET GANSE ORGANISATIE / TOUJOURS COMMUNICATION AVEC TOUTE L'ORGANISATION

DOLERO

alia
connecting security interests

Implementatie / Implementation

- Projectbewaking / Suivi de projet -- TEAM
  - Scope – Timing (Milestones) => Budget
- Testing
  - Dubbel werk : JA !! / Double boulot : OUI !!
  - Goede mix van gebruikers / Bon mix d’utilisateurs
  - Blijf bij de Scope / Reste chez le Scope
  - NO TESTING = NO GO
- Documentatie & Training / Documentation & Formation

Risico’s / Risques

- Implementatie van wat er al bestaat / Implémentation des choses qui existent déjà
- Out of Scope, Out of Timing = OUT OF BUDGET
- Organisatie kent het doel niet / Organisation ne connait pas l’objectif
- Ontevredenheid / Insatisfaction
- PROJECT FAIL

Samengevat / En Résumé

DOLERO

alia
connecting security interests

Patrick Van Liempt

INCERT Video: nieuwe T030/2 en globale risico analyse

INCERT Vidéo: nouveau T030/2 et l'analyse globale des risques

INCERT
CERTIFICATION

ALIA Security Day 2024
INCERT 2.0


INCERT : INTRUSION CERTIFICATION

Une marque de qualité volontaire pour la protection contre le vol

Een vrijwillig kwaliteitslabel voor de beveiliging tegen diefstal

INTRUSION INCERT CERTIFICATION

295

MONITORING INCERT CERTIFICATION

11

VEHICLES INCERT CERTIFICATION

60

VIDEO INCERT CERTIFICATION

10

alia
connecting security interests


Qui sommes-nous ?

INCERT : marque reconnue et soutenue par tous les acteurs du secteur de la sécurité depuis 2002

- Les compagnies d'assurance (ASSURALIA)
- Les Fédérations professionnelles de fabricants, les importateurs et les distributeurs (ACA, AGORIA Safety Technology, FEE Security, ELOYA, TECHLINK, NELECTRA, FEBIAC, TRAXIO)
- Les entreprises de consultance en sécurité autorisées (ISA-ICS)
- Les organismes de certification et de contrôle et les laboratoires compétents (ANPI, VINCOTTE, KIWA et IMQ)
- Les courtiers d'assurance (FEPRABEL)

Wie zijn wij?

INCERT: erkend en gesteund door alle actoren van de beveiliging sinds 2002

- Verzekeringsmaatschappijen (ASSURALIA)
- Beroepsfederaties van fabrikanten, importeurs en bedrijven (ACA, AGORIA Safety Technology, FEE Security, ELOYA, TECHLINK, NELECTRA, FEBIAC, TRAXIO)
- Vergunde ondernemingen voor veiligheidsadvies (ISA-ICS)
- Certificerings- en controle-instanties en bevoegde laboratoria (ANPI, VINCOTTE, KIWA en IMQ)
- Verzekeringsmakelaars (FEPRABEL)


La plus-value d'un installateur certifié INCERT

- Une analyse de risque approfondie (INCERT 125)
- Une offre de prix détaillée :
  - niveau de risque théorique et réel
  - concept de l'installation
  - informations légales
- Une installation selon les règles de l'art et la note technique INCERT T015/2
- Des produits certifiés INCERT
- Des audits annuels par un organisme de contrôle
- Un certificat de conformité INCERT
- Un engagement de performance !

De meerwaarde van een INCERT gecertificeerde installateur

- Een doorgedreven risico analyse (INCERT 125)
- Een gedetailleerde offerte:
  - theoretisch en gerealiseerd risico niveau
  - concept van de installatie
  - wettelijke info
- Een installatie volgens de regels van de kunst en volgens de technische nota INCERT T015/2
- INCERT gecertificeerde producten
- Jaarlijkse audits door een controle organisme
- Een INCERT conformiteitsverklaring
- Een resultaatsverbintenis!

alia
connecting security interests

Une inspection selon la T015/2 ne constitue pas une déclaration de conformité INCERT !

- Il s'agit uniquement d'un contrôle visuel et fonctionnel de l'installation basé sur la T015/2
- Qu'en est-il de l'analyse et le niveau de risque ?
- Une déclaration de conformité ne peut être émise que par un installateur certifié INCERT
- Qu'en est-il de la fiabilité de l'installateur ?
  - Assurance RC
  - Structure
  - Service après-vente
  - Audit annuel
  - ...
- Qu'en est-il de l'entretien annuel de l'installation ?

Een controle volgens de T015/2 is géén INCERT conformiteitsverklaring!

- Het gaat enkel om een visuele en functionele controle van de installatie op basis van de T015/2
- Hoe zit het met de risicoanalyse en het risiconiveau?
- Een conformiteitsverklaring kan enkel door een INCERT gecertificeerde installateur uitgeschreven worden
- Hoe zit het met de betrouwbaarheid van de installateur?
  - Verzekering BA
  - Structuur
  - Dienst na verkoop
  - Jaarlijkse audit
  - …
- Hoe zit het met het jaarlijks onderhoud van de installatie?

alia
connecting security interests

La marque mérite une plus grande notoriété

- Affiches INCERT
- Quote cards sur notre site et LinkedIn
- Campagne Google Ads
- Un site web plein d'informations
- Webinaires de (in)formation(s)
- Bulletins d'informations aux installateurs
- Bulletins d'information des nouveaux produits certifiés
- Promotion de la marque auprès des conseillers en prévention, les bureaux d'étude et les courtiers en assurances (Webinar, newsletter, meeting)
- Communication par l'installateur certifié (véhicules, site web, offres, …)

Het merk verdient meer naambekend

- Posters INCERT
- Quote cards op onze site en LinkedIn
- Google Ads campagne
- Een website boordevol informatie
- Vorming en informatie webinars
- Nieuwsbrieven aan de installateurs
- Nieuwsbrieven voor nieuwe gecertificeerde producten
- Promotie van het merk bij preventie adviseurs, studieburelen en verzekering makelaars (Webinars, newsletter, meetings)
- Communicatie door de gecertificeerde installateur (voertuigen, website, offertes, …)

alia
connecting security interests

INCERT
CERTIFICATION

INCERT VIDEO T030/2


Pourquoi une certification INCERT VIDEO ?

- Un installateur de systèmes de caméras doit être agréé, mais il n'y a pas (encore) de conditions techniques
- Avec la numérisation des systèmes de caméras (IP), de nouveaux acteurs (informatiques) apparaissent sur le marché
- Un système de caméras devient un système de sécurité et doit donc faire l'objet d'une analyse de risque approfondie
- Trop d'installations de caméras ne répondent pas aux attentes
- **Un certificat de qualité se justifie !**

Waarom een INCERT VIDEO certificatie?

- Een installateur camera systemen moet vergund zijn maar er zijn (nog) geen technische voorwaarden
- Met de digitalisering van de camerasystemen (IP) krijgen we nieuwe (IT)spelers op de markt
- Een camera systeem evolueert naar een beveiligingssysteem en daarom dient een grondige risico analyse uitgevoerd te worden
- Teveel camera installaties voldoen niet aan de verwachtingen
- **Een kwaliteitscertificaat dringt zich op!**

alia
connecting security interests


L'installateur certifié INCERT Vidéo (règlement 130)

- Est un installateur agréé pour systèmes de caméras
- Est audité par un organisme de certification
- Travaille toujours conformément à la norme T030/2
- A 2 spécialistes INCERT vidéo et du personnel qualifié sur le payroll
- Signe un engagement avec un ou plusieurs distributeurs vidéo certifiés
- A une entreprise saine et structurée, dotée d'une organisation solide en termes de planification, d'installation, de maintenance et de service après-vente
- Est bien documenté
- Entretient toutes ses installations annuellement
- Délivre un certificat de conformité pour chaque installation

De Incert Video gecertificeerde installateur (reglement 130)

- Is een vergund installateur camera systemen
- Wordt geauditeerd door een certificatie instelling
- Werkt steeds volgens de T030/2
- Heeft 2 INCERT video specialisten en gekwalificeerd personeel op de payroll
- Gaat een verbintenis aan met één of meerdere gecertificeerde video verdeler(s)
- Heeft een gezonde, gestructureerde onderneming met een degelijke organisatie qua planning, installatie, onderhoud en dienst na verkoop
- Is goed gedocumenteerd
- Zal zijn installaties jaarlijks onderhouden
- Levert voor elke installatie een conformiteitsverklaring

alia
connecting security interests


Pourquoi un une nouvelle note technique T030/2 ?

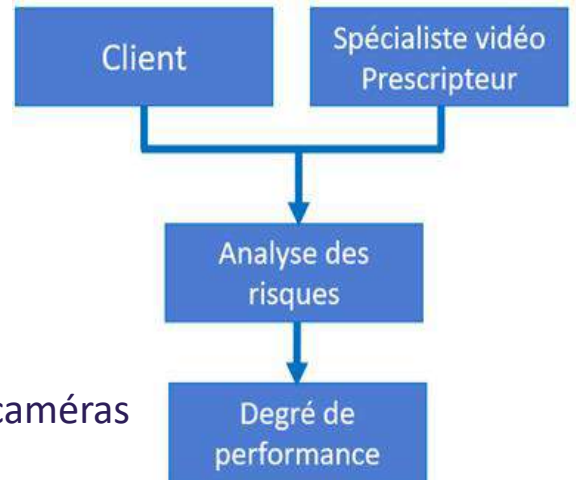
- Première version de 2015
- Évolution des technologies telles que les produits, les logiciels et l'analyse vidéo
- Nouvelles connaissances qui ont rendu nécessaire une mise à jour approfondie
- Construction structurelle du processus par un groupe de travail composé de spécialistes et d'experts en la matière

Waarom een nieuwe technische nota T030/2?

- Eerste versie van 2015
- Evolutie van de technologie zoals producten, software een video analyse
- Nieuwe inzichten waardoor een grondige update noodzakelijk werd
- Structurele opbouw van het proces door een werkgroep van specialisten en ervaringsdeskundigen


Une structure chronologique des différentes étapes du processus

- Détermination des besoins et de l'objectif du système
- L'analyse des risques
  - Valeur en cas de perte
  - L'emplacement
  - L'occupation
  - L'historique
  - Fonctions des caméras et du système de caméras
- Résultat : détermination des degrés de performance des caméras
- A ne pas confondre avec les niveaux de risque INCERT Intrusion



Een chronologische opbouw van de verschillende stappen van het proces

- Bepaling van de behoeften en doel van het systeem
- De risico analyse
  - Waarde bij verlies
  - Locatie
  - Bezetting
  - Geschiedenis
  - Functies van de camera’s en het camerasysteem
- Resultaat: bepaling van de prestatiegraden van de camera’s
- Niet te verwarren met de risico niveaus INCERT Intrusion


Les degrés de performance

- En fonction de la probabilité et des conséquences possibles d'un incident
- Sont déterminées par caméra
- P1 minimum : faible probabilité, faibles conséquences
- P2 moyen : probable, peu de conséquences
- P3 élevé : faible probabilité, conséquences importantes
- P4 très élevé : probable, conséquences importantes
- Le degré de performance de la caméra le plus élevé défini le degré de performance

De prestatiegraden

- Volgens de waarschijnlijkheid en de mogelijke gevolgen van een incident
- Worden bepaald per camera
- P1 minimum: weinig waarschijnlijk, weinig gevolgen
- P2 gemiddeld: waarschijnlijk, weinig gevolgen
- P3 hoog: weinig waarschijnlijk, belangrijke gevolgen
- P4 zeer hoog: waarschijnlijk, belangrijke gevolgen
- De hoogste prestatiegraad van de aangesloten camera’s bepaald de prestatiegraad van de centrale apparatuur


L'application de la caméra

De camera toepassing

Application de la caméra Camera toepassing	Pixels/m Valeur minimale Pixels/m Minimum waarde	Nbre minimal d'images par seconde * Minimum aantal beelden per seconde*	Mm/pixel Valeur maximale Mm/pixel maximumwaarde
Surveillance/bewaking	12	2	80
Détection/detectie	25	6	40
Observation/observatie	62	6	16
Reconnaissance/herkenning**	125	6	8
Identification/identificatie**	250	12,5	4
Inspection/inspectie**	1000	12,5	1

* Eventuellement plus selon la vitesse de déplacement/eventueel meer afhankelijk van bewegingssnelheid

**Eventuellement plus selon le risque/eventueel meer volgens het risico

connecting security interests


Conception du système : sélection des composants selon les degrés de performance

Ontwerp van het systeem: keuze van de componenten volgens de prestatie graden

	Spécifications	Degré de performance 1	Degré de performance 2	Degré de performance 3	Degré de performance 4
1	Exigences légales	O	O	O	O
2	Caméras intérieures Résistance aux chocs pour les caméras IK 10 + raccordement	-	R	-	O
3	Caméras extérieures Résistance aux chocs pour les caméras IK 10 + raccordement	-	R	R O à une hauteur inférieure à 3,5 m	O
4	Caméras extérieures Protection mécanique du câblage	R	O	O	O
5	Protection contre l'escalade	-	-	R	O
6	Installation de l'équipement d'enregistrement dans un local sécurisé	R	R	O en cas d'absence d'occupation permanente du lieu	O en cas d'absence d'occupation permanente dans le local de l'équipement d'enregistrement


	Specificaties	Prestatie-graad 1	Prestatie-graad 2	Prestatie-graad 3	Prestatie-graad 4
1	Wettelijke eisen	V	V	V	V
2	Binnencamera's Schokbestendigheid voor IK10-camera's + aansluiting	-	A	-	V
3	Buitencamera's Schokbestendigheid voor IK10-camera's + aansluiting	-	A	A V op een hoogte lager dan 3,5 m	V
4	Buitencamera's Mechanisch bescherming van de bekabeling	A	V	V	V
5	Inklimbeveiliging	-	-	A	V
6	Plaatsing van de opnameapparatuur in een beveiligd lokaal	A	A	V indien geen permanente bezetting van de plaats	V indien geen permanente bezetting van het lokaal van de opname apparatuur


Suite de la construction du processus

- Préparation de l'installation
- Installation du système de caméra
- Réception du système de caméra
  - Vérification
  - Formation
  - Réception
- Le dossier technique
- Exigences minimales pour la maintenance du système

Verdere opbouw van het proces

- Voorbereiding van de installatiewerken
- Installatie van het camerasysteem
- Oplevering van het camerasysteem
  - Controle
  - Opleiding
  - Oplevering en ontvangst
- Het technisch dossier
- Minimale vereisten voor het onderhoud van het systeem


Des annexes utiles

- L'offre
- L'analyse de risque
- Proof of concept (POC)
- La réalisation de l'installation
- Le dossier « As-Built »
- Estimation de la capacité de stockage réelle
- Inspections visuelles et fonctionnelles
- Vérification et livraison du système de caméras
- Matrice d'attribution des degrés de performance

Nuttige bijlagen

- De offerte
- De risico analyse
- Proof of concept (POC)
- Realisatie van de installatie
- Het As-Built dossier
- Schatting reële opslagcapaciteit
- Visuele en functionele inspecties
- Controle en oplevering camerasysteem
- Matrix voor de toekenning van de prestatie graden


Les prochaines étapes

- Publication et vente de la nouvelle T030/2 par le biais du NBN (Q2)
- Présentation et promotion auprès des parties prenantes et des installateurs (Q2)
- Adaptation de l'examen du spécialiste INCERT Vidéo (Q3)
- Formation de mise à jour obligatoire pour les spécialistes INCERT Vidéo (Q3)

De volgende stappen

- Publicatie en verkoop van de nieuwe T030/2 via NBN (Q2)
- Presentatie en promotie naar de stakeholders en installateurs (Q2)
- Aanpassing van het examen specialist INCERT Video (Q3)
- Verplichte bijscholing van de specialisten INCERT Video (Q3)


Avec nos remerciements au groupe de travail
Met dank aan de werkgroep

- Danny Hermans – VOLTA – Voorzitter/Président
- Patrick Van Liempt – ALIA
- Bernard Desmet – ASSURALIA
- Hugues Forest – TRACTEBEL
- Ronny Nedergedaelt – ANPI
- Thierry De Leeuw - ANPI
- Michel Verstraelen – IBS SECURITY
- Johan Chenot – SECURITAS
- Gino Van Der Ven – VINÇOTTE
- Jean-Pierre Derni – ISA
- Philippe Delwiche – RAS
- Ronald Koeck – G4S
- Sabine Vermeulen – CEB-BEC

alia
connecting security interests

INCERT
CERTIFICATION

Thank You

Jort Stassen

Evoluties van de norm NBN S21-100

Evolutions de la norme NBN S21-100

INHOUDSTAFEL / AGENDA

- Huidige toestand reeksen NBN S21-100 en NBN S21-111
- Toekomstige toestand: NBN S21-100 en NBN S21-112
- Selectiecriteria, uitleg over NBN S21-112-1
- Nieuwe werkgroep ‘Integratie’

- Situation actuelle des séries de normes NBN S21-100 et NBN S21-111
- Situation future: NBN S21-100 et NBN S21-112
- Critères de sélection, explication NBN S21-112-1
- Nouveau groupe de travail ‘Intégration’

ANPI

alia
connecting security interests

HUIDIGE TOESTAND / SITUATION ACTUELLE

Normenreeks NBN S21-100: Branddetectie- en brandmeldsystemen

- NBN S21-100-1 (2021):*Regels voor de risicoanalyse en de evaluatie van de behoeftes, de studie en het ontwerp, de plaatsing, de indienststelling, de controle, het gebruik, het nazicht en het onderhoud.*
- NBN S21-100-2 (2015): *Kwalificaties en competenties*

Séries de normes NBN S21-100: Systèmes de détection et systèmes d'alarme incendie

- NBN S21-100-1 (2021):*Règles relatives à l'analyse des risques et à l'évaluation des besoins, à l'étude et à la conception, à l'installation, à la mise en service, au contrôle, à l'utilisation, à l'inspection et à l'entretien.*
- NBN S21-100-2 (2015): *Qualifications et compétences*

ANPI

alia
connecting security interests

HUIDIGE TOESTAND / SITUATION ACTUELLE

Normenreeks NBN S21-111: Spraakalarmsystemen

- NBN S21-111-1 (2017): *Selectiecriteria*
- NBN S21-111-2 (2020): *Regels voor de studie, het ontwerp en de plaatsing*
- NBN S21-111-3 (2020): *Beheer, kwalificaties en competenties*

Série de normes NBN S21-111 : Systèmes d'alarme vocale

- NBN S21-111-1 (2017) : Critères de sélection
- NBN S21-111-2 (2020) : Règles d'étude, de conception et d'installation
- NBN S21-111-3 (2020) : Gestion, qualifications et compétences

ANPI

alia
connecting security interests

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

NBN S21-100-* & NBN S21-112-*

ANPI

alia
connecting security interests

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

DISCLAIMER

- Het betreft aanpassingen die momenteel verwerkt en voorgesteld zullen worden. Deze zijn pas definitief na publicatie.

AVIS DE NON-RESPONSABILITÉ

Il s'agit d'ajustements qui sont en cours de traitement et qui seront présentés. Ils ne seront définitifs qu'après publication.

ANPI

alia
connecting security interests

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

NBN S21-100-1

- Inhoudelijke veranderingen :

- Video Fire detection : Detectie van rook of vuur via optische beeldanalyse: installatierichtlijnen
- Risico-analyse : Versimpeld versie voor gebouwen met beperkt risico
- Valse alarmen : Uitleg en waarmee rekening te houden
- Aanpassing/uitbreiding : Wat is een aanpassing/uitbreiding van een brandmeldsysteem en waaraan moet worden voldaan.
- Sirenes : Verdwijnen integraal uit deze norm

NBN S21-100-1

- Principales modifications du contenu :

- Implémentation de la technologie « Video Fire detection »: Détection de fumée ou de flamme par le biais d'une image optique : directives d'installation
- Analyse de risque : ajout d'une version simplifiée pour les bâtiments à faible risque
- Fausses alarmes : considérations supplémentaires sur les éléments à prendre en considération
- Modification/extension : Qu'est-ce qu'une modification/extension d'un système d'alarme incendie et que faut-il respecter ?
- Sirènes : disparaissent complètement de cette norme

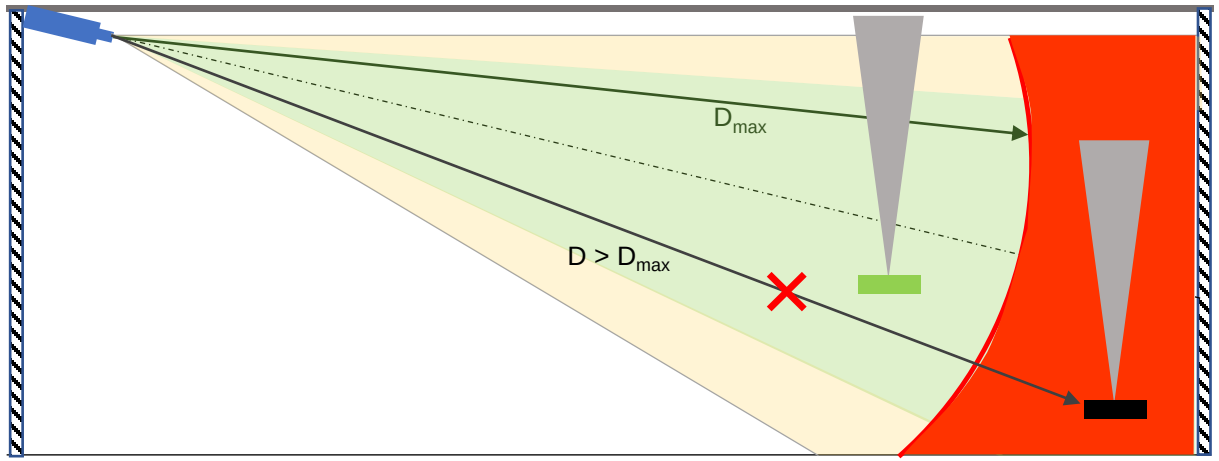
ANPI

alia
connecting security interests

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

NBN S21-100-1

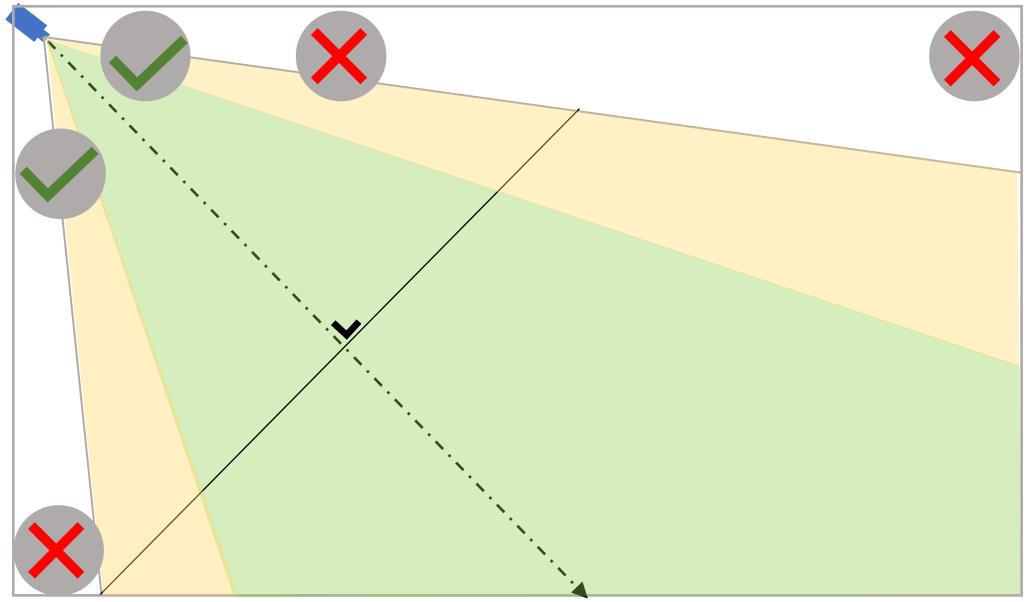
- Video Fire detection:
  - Duidelijke eisen inzake:
    - Inplanting en oriëntatie van de camera
    - Achtergrondverlichting
    - Beeld en eventueel toegestane (beperkte) blinde vlekken
  - ...



Zijaanzicht - coupe

NBN S21-100-1

- Détection d'incendie par vidéo:
  - Exigences claires en matière :
    - d'emplacement et d'orientation de la caméra
    - d'éclairage d'ambiance
    - d'image et d'éventuels angles morts autorisés (limitation)



Bovenaanzicht - vue en plan

ANPI

alia
connecting security interests

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

Normenreeks NBN S21-111

- Houdt op te bestaan.
- Zal worden overgeplaatst naar een nieuwe normenreeks NBN S21-112 (Branddetectie- en brandmeldsystemen – Alarmsystemen)

Série de normes NBN S21-111

- Cessera d'exister.
- Sera transférée dans une nouvelle série de normes NBN S21-112 (Systèmes de détection et d'alarme incendie - Systèmes d'alarme)

ANPI

alia
connecting security interests

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

Normenreeks NBN S21-112

Nieuwe structuur:

- NBN S21-112-1: *Selectiecriteria*
- NBN S21-112-2: *Beheer, kwalificaties en competenties*
- NBN S21-112-3: *Alarmsystemen met akoestische signaalgevers: Regels voor de studie, het ontwerp, de plaatsing, de indienststelling, de controle, het gebruik, het nazicht en het onderhoud*
- NBN S21-112-4: *Spraakalarmsystemen: Regels voor de studie, het ontwerp, de plaatsing, de indienststelling, de controle, het gebruik, het nazicht en het onderhoud*
- *NBN S21-112-5: ???*

Série de normes NBN S21-112

Nouvelle structure :

- NBN S21-112-1 : Critères de sélection
- NBN S21-112-2 : Gestion, qualifications et compétences
- NBN S21-112-3 : Systèmes d'alarme avec générateurs de signaux acoustiques : Règles d'étude, de conception, d'installation, de mise en service, de contrôle, d'exploitation, d'entretien et de maintenance
- NBN S21-112-4 : Systèmes d'alarme vocale : Règles d'étude, de conception, d'implantation, de mise en service, de contrôle, d'exploitation, d'inspection et de maintenance
- NBN S21-112-5 : ? ???

TOEKOMSTIGE TOESTAND / SITUATION FUTURE

NBN S21-112-1 Selectiecriteria:

Nieuwe aanpak risicoanalyse:

- voor diverse signaalgevers gecombineerd
- gestructureerde vragenlijst
- nota's met belangrijkste aandachtpunten
- logische indeling

NBN S21-112-1 Critères de sélection :

Nouvelle approche de l'analyse des risques :

- pour différents générateurs de signaux combinés
- questionnaire structuré
- notes avec les principaux points d'attention
- classification logique

ANPI

alia
connecting security interests

NBN S21-112-1

Selectiecriteria

Critères de sélection

ANPI

alia
connecting security interests

NBN S21-112-1 Selectiecriteria - Critères de sélection

- Het project
  - Bouwwerk en omgeving
  - Personen
  - Risicoprofiel bouwwerk en omgeving
- Toepasselijke voorschriften alarmsignalering
- Noodsituaties
  - Welke?
  - Strategie?
  - Waar?

- Le projet
  - Structure et environnement
  - Les personnes
  - Profil de risque de la structure et de son environnement
- Réglementation applicable en matière d'alarme
- Situations d'urgence
  - Lesquelles ?
  - Stratégie ?
  - Où ?

ANPI

alia
connecting security interests

NBN S21-112-1 Selectiecriteria - Critères de sélection

Hoe kenbaar maken

- Signalisatie in functie van aanwezige personen
- Relevante omgevingsfactoren
- Aanvullende signaalgevers?

Waarneembaarheid en kenbaarheid van alarmsignalen

Goed herkenbaar/waarneembaar en zonder verwarring

Comment signaler

- Signalisation en fonction des personnes présentes
- Facteurs environnementaux pertinents
- Dispositifs de signalisation supplémentaires ?

Détection et reconnaissance des signaux d'alarme

Bien reconnaissables/perceptibles et sans confusion

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

4.2 Vragenlijst

4.2.2 Beschrijving van het project

1.De bouwwerken en/of hun omgeving
-Welke bouwwerken en/of hun omgeving maken deel uit van het project?

-Wat is de configuratie van de bouwwerken en hun omgeving?

Nota: denk aan hoogte, uitgestrektheid, complexiteit, stabiliteit bij brand, compartimentering, reactie bij brand van materialen, …;

Nota voor plaatsen buiten: denk aan arbeidsplaatsen, binnenkoer, speelplaats, campus, dakterras, bedrijfsterrein, tot openbare weg, …

-Wat is de configuratie van de evacuatiewegen?

Nota: denk aan capaciteit, lengte, complexiteit, bescherming (b.v. al dan niet brandwerend omsloten), …;

-Welke andere brandbeschermingsmaatregelen (actief en/of passief) kunnen een invloed hebben op de keuze van de alarmsystemen? (compartimentering, automatische blussystemen, rook- en warmteafvoersystemen, …);

-Vermeld indien nodig ook andere relevante elementen.

4.2 Questionnaire

4.2.2 Description du projet

1. Les structures et/ou leur environnement
- Quelles sont les structures et/ou leur environnement qui font partie du projet ?
- Quelle est la configuration des structures et de leur environnement ?

Note: tenir compte de la hauteur, de l'étendue, de la complexité, de la stabilité en cas d'incendie, du compartimentage, de la réaction au feu des matériaux, ...;

Note pour les lieux extérieurs : pensez aux lieux de travail, cours intérieures, aires de jeux, au campus, terrasses de toit, terrain d'entreprise, jusqu'à la voie publique, ...

-Quelle est la configuration des voies d'évacuation ?

Note : tenez compte de la capacité, de la longueur, de la complexité, de la protection (par exemple, enceinte ignifugée ou non), ...

- Quelles autres mesures de protection contre l'incendie (actives et/ou passives) peuvent influencer le choix des systèmes d'alarme ?(compartimentage, systèmes d'extinction automatique, systèmes d'extraction de fumée et de chaleur, ...)

-A jouter d'autres éléments pertinents si nécessaire

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

2. De aanwezige personen

- Welke types personen zijn aanwezig?

Nota: denk aan zelfredzaam / niet zelfredzaam, slapend / wakend, vertrouwd / niet vertrouwd, … geef voldoende informatie bij niet zelfredzame personen, b.v. gaat het om fysieke en/of psychische factoren die de niet zelfredzaamheid veroorzaken, permanent of tijdelijk, …?

- In welke aantallen zijn deze aanwezig?

- Waar in de gebouwen en/of hun omgeving zijn deze aanwezig?

2. Les personnes présentes

- Quels types de personnes sont présentes?

Note : considérez les personnes autonomes/non autonomes, dormantes/vigilantes, de familiarisées / non familiarisées,.... fournissez des informations suffisantes dans le cas de personnes non autonomes, par exemple, des facteurs physiques et/ou psychologiques sont-ils à l'origine de l'absence d'autonomie, permanente ou temporaire,... ?

- Quel est leur nombre ?

- Où se trouvent-elles dans les bâtiments et/ou leurs environs ?

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

3. Beschrijf het risicoprofiel van de bouwwerken en/of hun omgeving

Nota: denk hierbij bijvoorbeeld aan de volgende punten

- Risico's van bijzondere aard: een energiecentrale, een kerncentrale, een SEVESO-bedrijf, …;

- Met aanwezigheid van gevaarlijke producten

- Het mogelijke gebruik van het bouwwerk, de polyvalentie in uitbating, de evolutie in de tijd, …;

- Met een potentieel grote concentratie aan personen: metro- en/of treinstations, luchthavens, sportstadions, scholen, universiteiten, evenementen, …;

- Terrorismegevoeligheid;

- Eventueel andere relevante elementen.

3. Décrire le profil de risque des structures et/ou de leur environnement

Note: considérer, par exemple, les points suivants

- Risques de nature particulière : une centrale électrique, une centrale nucléaire, une entreprise SEVESO, ...;

- Avec la présence de produits dangereux ;

- L'utilisation possible de la structure, sa polyvalence de fonctionnement, son évolution dans le temps, etc.

- Avec une concentration potentiellement importante de personnes : stations de métro et/ou gares, aéroports, stades, écoles, universités, événements, ... ;

- Sensibilité au terrorisme ;

- Eventuellement d'autres éléments pertinents.

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

4.2.2.Welke zijn de toepasselijke voorschriften op het bouwwerk en zijn omgeving in verband met alarmsignalering?

Nota: geef een overzicht van de relevante regelgeving, normen en andere voorschriften zoals vergunningsvoorwaarden, adviezen van de brandweer, regels van goede praktijk, ...

4.2.2. Quelles sont les réglementations applicables à la structure et à son environnement en matière de signalisation d'alarme?

Note : dressez la liste des réglementations, normes et autres exigences pertinentes, telles que les conditions d'obtention d'un permis, les avis des pompiers, les règles de bonne pratique, etc.

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

4.2.3. Noodsituaties: voor welke noodsituaties is er alarmsignalering nodig in dit project?

1.Welke noodsituaties zijn van toepassing**?**
Voorbeelden: brand, chemisch probleem, amok, terrorisme, …

2.Welke strategie of plan van aanpak wordt gebruikt per noodsituatie?

Nota: dit betekent ook het bepalen van het gewenste gedrag in functie van een bepaalde noodsituatie

Nota: welke stappen / fases, algemene evacuatie, gefaseerde evacuatie, defend in place, binnen blijven of barricaderen, naar veilige plaats gaan in het gebouw, horizontale evacuatie, …

Nota: kan de evolutie van een noodsituatie leiden tot een evolutie van de noodsignalen? (b.v. opschalen of afbouwen, andere fase, …)
Voorbeeld: bij brand spreekt de regelgeving typisch van ontdekking, waarschuwing, melding, alarm (evacuatie).

3.Waar moeten die noodsituaties gesignaleerd worden? (plaats, alarmzone, binnen, buiten, …)

a) In welke bouwwerken en/of omgeving moet welke noodsituatie gesignaleerd worden?

b) Wat is de indeling in alarmzones van de bouwwerken en/of hun omgeving?

Nota: kunnen deze noodsituaties zich lokaal of algemeen voordoen? Waar signaleren in functie daarvan? Denk eraan dat de indeling in alarmzones verschillend kan zijn in functie van de noodsituaties.

4.2.3. Situations d'urgence : pour quelles situations d'urgence des alarmes sont-elles nécessaires dans le projet ?

1. Quelles sont les situations d'urgence applicables ?
Exemples : incendie, problème chimique, fuite, terrorisme,...

2. Quelle stratégie ou quel plan d'action est utilisé pour chaque situation d'urgence ?

Note : il s'agit également de déterminer le comportement souhaité en fonction d'une situation d'urgence particulière.

Note: quelles étapes/phases, évacuation générale, évacuation par étapes, se défendre sur place, rester à l'intérieur ou se barricader, se mettre en lieu sûr dans le bâtiment, évacuation horizontale, etc.

Note : l'évolution d'une situation d'urgence peut-elle entraîner une évolution des signaux d'urgence ? (Exemple : dans le cas d'un incendie, la réglementation prévoit généralement la découverte, l'alerte, l'annonce et l'alarme (évacuation).

3. Où ces urgences doivent-elles être signalées ? (lieu, zone d'alarme, intérieur, extérieur,...)
a) Dans quels bâtiments et/ou leurs environs doit-on signaler quelle situation d'urgence ?
b) Quelle est la classification de la zone d'urgence des bâtiments et/ou de leur environnement ?

Note : cette situation d'urgence peut-elle se produire localement ou de manière générale ?
Où signaler en fonction de cette situation ?
N'oubliez pas que les zones d'alarme peuvent varier en fonction des situations d'urgence.

ANPI

alia
connecting security interests

VRAGEN-QUESTIONS NBN S21-112-1

4.2.4.Hoe de noodsituatie kenbaar maken? (type signaal)

Bij de keuze van het signaal moet rekening worden gehouden met de volgende factoren en met de types signaalgevers.

1.Beschrijf de signalisatie in functie van de aanwezige personen. (zie ook § 4.2.1)

a) Wat is hun rol of taak: personeel al dan niet met een specifieke taak in geval van nood, bezoeker, bewoner, …?

b) Voor wie is het signaal bedoeld?

Nota:

- moet iedereen het signaal kunnen waarnemen en begrijpen of alleen specifieke personen?
- hoe reageren de verschillende types personen op de signalen? Zijn er b.v. niet zelfredzame personen waarbij een luid signaal voor paniek kan zorgen?

4.2.4 Comment communiquer l'urgence ? (type de signal)

Les facteurs suivants doivent être pris en compte lors du choix du signal et des types de dispositifs de signalisation.

1.Décrire la signalisation en fonction des personnes présentes (voir aussi 4.2.1)

a) Quel est leur rôle ou leur tâche : personnel ayant ou non une tâche spécifique en cas d'urgence, visiteur, occupant,... ?

b) À qui le signal est-il destiné ?

Note :

- Tout le monde doit-il être en mesure de percevoir et de comprendre le signal ou seulement certaines personnes ?
- Comment les différents types de personnes réagissent-ils aux signaux ?

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

2. Beschrijf de relevante omgevingsfactoren (zie ook 4.2.1)
a. Factoren met invloed reactietijd/uitvoeringstijd: afstanden, capaciteit, complexiteit, middelen/systemen
(beveiligingssystemen, verlihcting, signalisatie,…), te verwachten risico's (rookontwikkeling, hitte, puin, gevaarlijke personen,…)
b. Type activiteit(en): industrie, school, shopping, zorg, kantoor,…
c. Omgevingsfactoren zoals lawaai, verlichting, zichtbaarheid,…

Nota: in de zones waar de geluidsignalen slecht hoorbaar zijn, bijvoorbeeld omwille van overmatig achtergrondlawaai, moeten alternatieve oplossingen voorzien worden zoals naast de geluidsignalen ook visuele en/of tactiele signale plaatsen.

3. Zijn aanvullende signaalgevers nodig? Zo ja, welk type en waar?

2. Décrire les facteurs environnementaux pertinents (voir aussi 4.2.1)

a) Facteurs influençant le temps de réaction/d'exécution : distances, capacité, complexité, moyens/systèmes (systèmes de sécurité, éclairage, signalisation,...), risques prévisibles (dégagement de fumée, chaleur, débris, personnes dangereuses,...).
b) Type d'activité(s) : industrie, école, magasins, soins, bureau,...
c) Facteurs environnementaux tels que le bruit, l'éclairage, la visibilité,...

Note : dans les zones où les signaux sonores sont difficiles à entendre, par exemple en raison d'un bruit de fond excessif, il convient de prévoir des solutions alternatives telles que l'installation de signaux visuels et/ou tactiles en plus des signaux sonores.

3. Des dispositifs de signalisation supplémentaires sont-ils nécessaires ? Si oui, de quel type et à quel endroit ?

ANPI

alia
connecting security interests

VRAGENLIJST - QUESTIONNAIRE NBN S21-112-1

4.2.5 Waarneembaarheid en herkenbaarheid van de alarmsignalen
Zorg ervoor dat de alamrsignalen voor alle betrokken personen goed waarneembaar
en herkenbaar zijn en noch met elkaar, noch met andere signalen verward kunnen worden.
Nota: het doel van deze stap is waar mogelijk te vereenvoudigen en/of te uniformiseren zonder afbreuk te doen aan het vereiste resultaat.
-Gebruiken we voor elk type gewenst gedrag hetzelfde type signaal ?
-Wat zijn de onderlinge prioriteiten van de signalen?
-Is de zone-indeling zo eenvoudig mogelijk gemaakt?
-Is er een coherente aanpak over het evacuatietraject?

Nota : de keuze voor een flexibeler en/of polyvalenter systeem wordt interessanter naarmate:
-de lijst van noodsituaties en de erbij horende signalen en/of systemen langer wordt (meerdere situaties en/of signalen, live aanpasbare signalen,…)
-de noodistuaties kunnen evolueren in de tijd

4.2.5 Perceptibilité et reconnaissabilité des signaux d'alarme
Veillez à ce que les signaux d'alarme soient clairement perceptibles et reconnaissables pour toutes les personnes concernées et à ce qu'ils ne puissent pas être confondus entre eux ou avec d'autres signaux. et reconnaissables et qu'ils ne peuvent pas être confondus entre eux ou avec d'autres signaux**.**
Note: l'objectif de cette étape est de simplifier et/ou d'unifier dans la mesure du possible sans compromettre le résultat recherché.
-Utilise-t-on le même type de signal pour chaque type de comportement souhaité ?
-Quelles sont les priorités respectives des signaux ?
- la répartition des zones est-elle bien aussi simple que possible ?
- Y a-t-il une approche cohérente en ce qui concerne les chemins d'évacuation ?

Note : le choix d'un système plus flexible et/ou polyvalent devient plus intéressant au fur et à mesure que :
-la liste des situations d'urgence et des signaux et/ou systèmes associés s'allonge (situations et/ou signaux multiples, signaux adaptables en direct,...)
-les situations d'urgence peuvent évoluer dans le temps

ANPI

alia
connecting security interests

INTEGRATIE

NIEUWE WERKGROEP

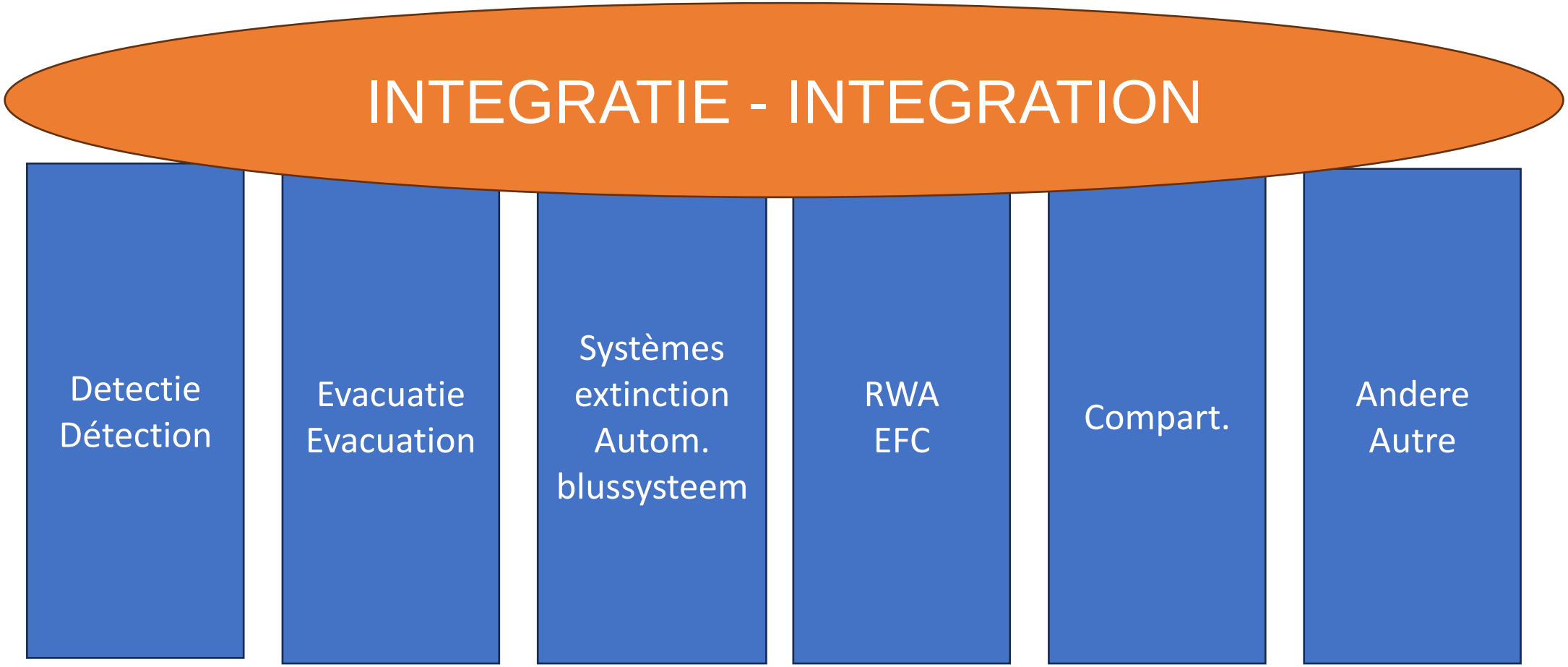
INTEGRATION

NOUVEAU GROUPE DE TRAVAIL

ANPI

alia
connecting security interests

GROUPE DE TRAVAIL INTEGRATION
WERKGROEP INTEGRATIE



ANPI

alia
connecting security interests

WERKGROEP INTEGRATIE
GROUPE DE TRAVAIL INTEGRATION

Doel: correcte werking tussen verschillende systemen garanderen

Bepalen van:

- eisen in verband met gebruikte materialen (gecertificeerd?)
- eisen in verband met overwakingen tussen verschillende technieken
- eisen in verband met betrouwbaarheid verbindingen (failsafe, functiebehoud, …)
- …
- …

Momenteel vage zone: duidelijkheid te scheppen via nieuwe norm

Objectif : assurer un fonctionnement correct entre les différents systèmes

Déterminer :
- les exigences relatives aux composants utilisés (certifiés ?)
- les exigences relatives aux surveillances de circuits entre les différentes techniques
- les exigences relatives à la fiabilité des connexions (sécurité intégrée, maintien de la fonction, ...)
- ...

Zone actuellement vague : à clarifier par le biais d'une nouvelle norme

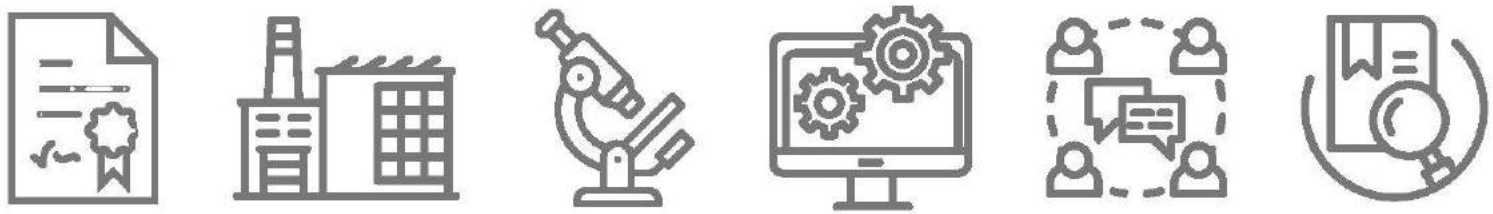
ANPI

alia
connecting security interests

BEDANKT VOOR JULLIE AANDACHT
MERCI POUR VOTRE ATTENTION

JORT STASSEN
ANPI
TOT UW DIENST – A VOTRE SERVICE

www.anpi.be info@anpi.be



ANPI

alia
connecting security interests

Benoit Stockbroeckx

Remote service en het gebruik van de Cloud

Service à distance et utilisation du Cloud

De 20ste eeuw

Le 20ème siècle

alia
connecting security interests

n systeem niet inschakelen

r mon système

Het Service Bezoek
L’intervention sur demande

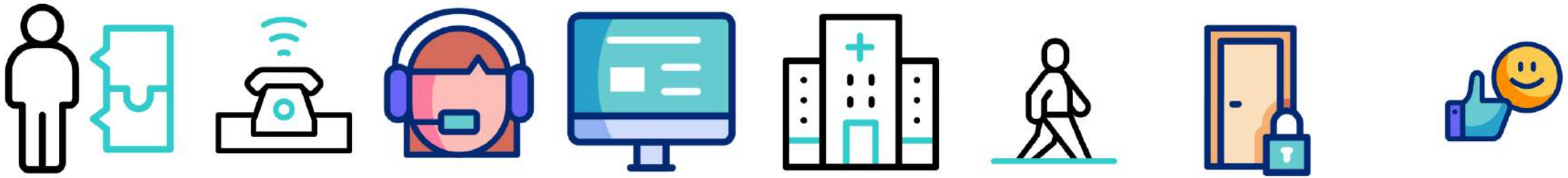
120 minuten / minutes

alia
connecting security interests

De 21ste eeuw

Le 21ème siècle

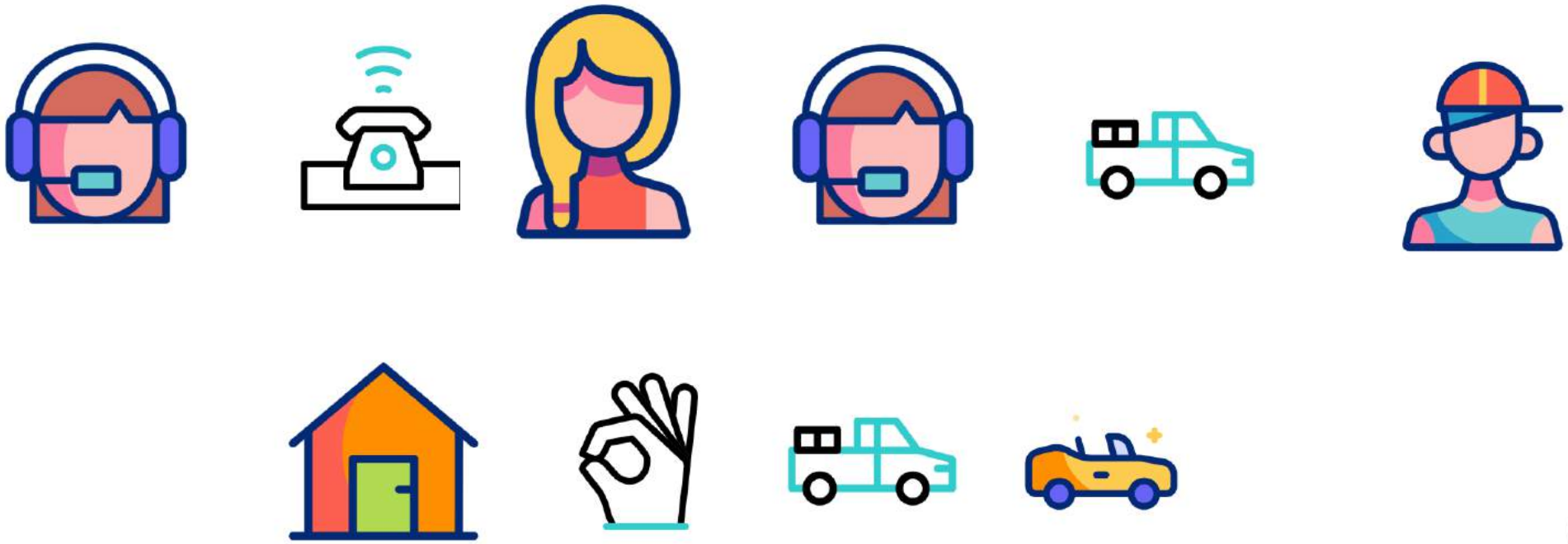
alia
connecting security interests



De Remote Service Call
Le service à distance

10 minuten / minutes

alia
connecting security interests



Het Onderhoud Bezoek
La visite de maintenance

120 minuten / minutes

OK, alles is in orde

OK, tout est en ordre

Het Remote Onderhoud
La maintenance à distance

10 minuten / minutes

alia
connecting security interests

Toegevoegde waarde

- Lagere kosten
- Betere klanten ervaring
- Beter voor milieu
- Minder verplaatsing

Valeur ajoutée

- Diminution des coûts
- Meilleure expérience client
- Meilleur pour l’environnement
- Moins de déplacements

alia
connecting security interests

Les bonnes pratiques
Correcte uitvoering

D’accord pour les services à distance

Qu’en est-il des règles de bonnes pratiques?

Overeenkomst voor diensten op afstand Hoe zit

het met de regels voor goede uitvoering?

- Elles guident les fournisseurs de services
- Ze ondersteunen dienstverleners

- Elles permettent l’acceptation par les utilisateurs, les assureurs et les services de secours
- Ze worden geaccepteerd door gebruikers, verzekeraars en hulpdiensten

- Elles permettent le développement de ce mode de services
- Ze maken de toepassing van dit soort diensten mogelijk

alia
connecting security interests

Les bonnes pratiques
Correcte uitvoering

	3 normes européennes	3 Europese normen
EN 16763	Prestations de services pour les systèmes de sécurité incendie et les systèmes de sûreté	Diensten voor brandveiligheids- en beveiligingssystemen
EN 50710	Lignes directrices et exigences relatives aux services à distance sécurisés pour les systèmes de protection incendie et les systèmes de sûreté	Vereisten voor het leveren van veilige diensten op afstand voor brandbeveiligingssystemen en beveiligingssystemen
CLC/TS 50136-10	Systèmes d'alarme - Systèmes et équipements de transmission d'alarme - Partie 10 : Exigences pour l'accès à distance	Alarmsystemen - Alarmtransmissiesystemen en -apparatuur - Deel 10: Vereisten voor toegang op afstand

alia
connecting security interests

Guide Euralarm disponible
Euralarm handboek beschikbaar

1 seul guide pour l'application conjointe des 3 normes, Novembre 2022

1 handboek voor de gezamenlijke toepassing van de 3 normen, November 2022

EN 16763

Prestations de services

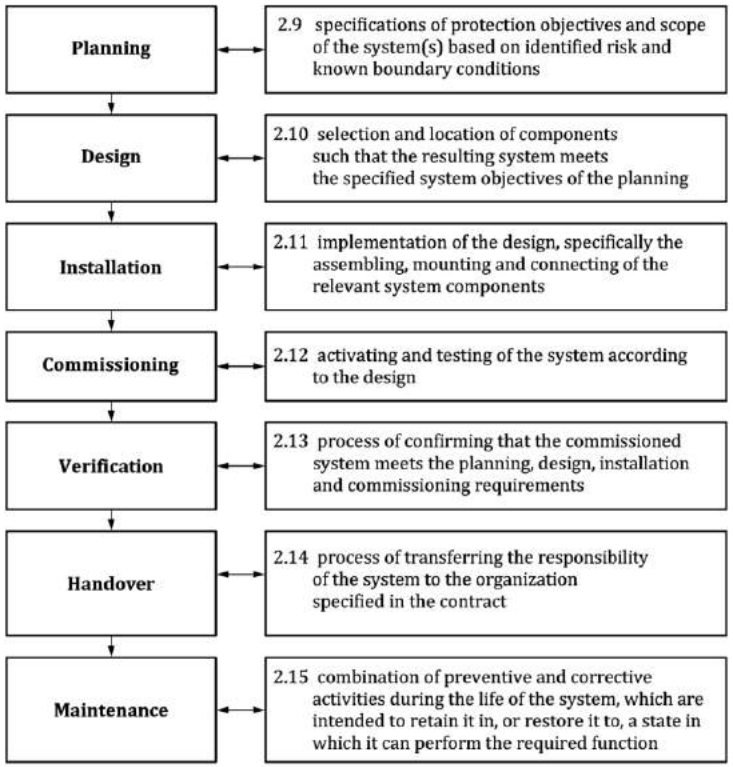


Figure 2 — Stages of work for fire safety systems and security systems

Diensten

EN 16763:2017 CEN-CLC TC4	Services for fire safety systems and security systems.		
	This standard specifies the minimum requirements for service providers as well as the competencies, knowledge and skills of their involved staff, regardless whether these services are provided on-site or remotely.		
	Requirement	Chapter	Check
General	*Note: Annex A for guidance on the documentation of the stages of work*	3.1	
	Identification of the service provider (name and trading name, address, authorized person, national registrations,...)	3.2	
	Meet national laws and regulations.	3.2	
	Use this standard requirements only in conjuction with EN standards and national guidelines.	3.2	
	Have resources, knowledge and skills to fulfill the declared services.	3.2	
	Processes to execute the declared services rightfully	3.2	
	Processes to record executed services and mantain these records.	3.2	
	Have executed services in the field of expertise	3.2	
	Initial and ongoing staff training	3.2	
	Insurance for all declared services	3.2	
	Management system that covers the quality of the execution of the declared services	3.2	
	Access to manufacturers' instructions for components and systems for the declared services	3.2	
	Access to the applicable standards, guidelines,...	3.2	
	Keep client related information confidential and secure	3.2	
	Where allowed by regulation and required, provide evidence of security vetting	3.2	
	Use components and systems complying with the existing standards and/or acknowledged rules of technology	3.2	
Subcontracting	Responsibility stays in the service provider	3.3	
	Processes to monitor and manage the quality of subsconstructed services	3.3	
Staff	Identify staff undertaking roles A,B,C	3.4	
	Demonstrate adequate numbers to support the service provided	3.4	
	Role A (decision-making authority + responsability for compliance). - level 5 of EQF within the declared services, or -realizing 3 systems in the last 5 years in the declared services	3.4	
	Role B (self management and supervision of the routine work of others, some responsibility for the evaluation and improvement of work). - level 4 of EQF within the declared services, or -realizing 3 systems in the last 3 years in the declared services	3.4	
	Role C (fullfilling assigned tasks in a reliable way). - level 3 of EQF	3.4	
Service output	Processes for defining and documenting the output of a stage of work: - alligned with the relevant application guide - in accordance with local requirements - change control - identify the responsible person	3.5	
	Requirements for maintenance providers: - staff with the right knowledge, skills and competences - maintenance in accordance with contract and manufacturer's specifications - service output in accordance with general requirements, client informed.	3.5	

alia
connecting security interests

Guide Euralarm disponible
Euralarm handboek beschikbaar

EN 50710 Services à distance Diensten op afstand

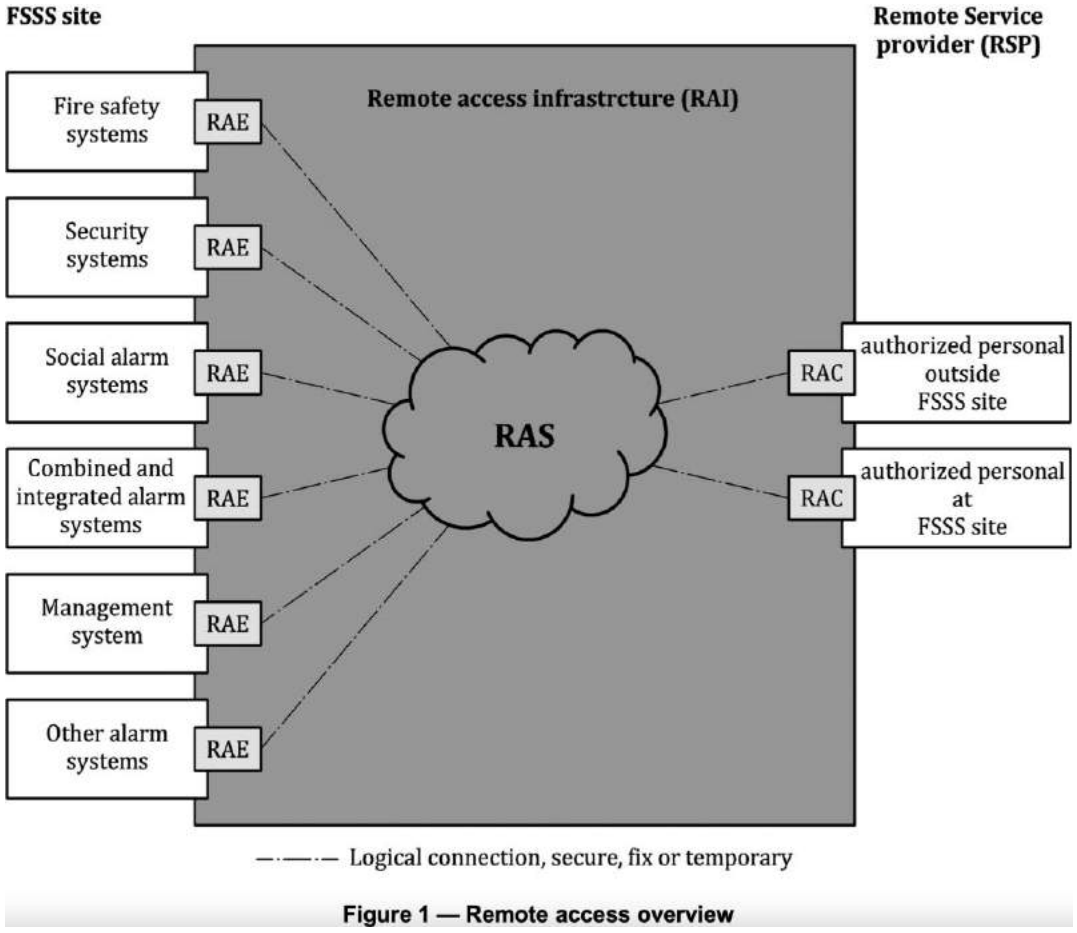


Figure 1 — Remote access overview

EN 50710:2021 CEN/CLC/JTC4	Remote Services for fire systems and security systems.		
	This standard specifies the minimum requirements for the provision of secure remote services via a remote access infrastructure carried out either at site or off-site. This standard is intented to support the implementation of the European Service Directive (2006/123/EC) and EN 16763 Services for fire safety systems and security systems.		
	Requirement	Chapter	Check
Service organization	Assessment of the risk added	4.1	
	Remote service processes, technologies and communication paths are secure and reliable (design, documentation and holistic testing)	4.1	
	Operation of remote services shall be informed (client, service provider*, MARC*, response authorities*)	4.6	
	Impact assessment of remote service before it is performed	4.6	
	Mitigation measures alligned with risk assessment during the remote service	4.6	
	Funcionality check after the remote service is performed	4.6	
	Remote service requirements are to be applied in conjunction with technical application guidelines	4.4	
RAI	RAI periodic testing, maintenance and update	4.1	
	Training to use RAI within service provider	4.1	
	RAI security supported by state of the art security measures (authentication, authorization, encryption, substitution protection, event logging, traceability).	4.3	
	RAI physical and logical connections monitored for cyber security.	4.3	
RAS	RAS and associated applications are located in -FSSS site, or -MARC (certified in EN50518), or -data centre (certified in EN50600). Service Organizations: certified in EN 16763.	4.3	
	Remote access to the FSSS only via RAS	4.3	
RAC	Authorization to access the RAC	4.3	
	RAC sessions automatic termination	4.3	
	Secure access to remote service: - authorized persons per specific operation, list periodically reviewed - access terminals proper location - session automatic termination - connection to RAS is secure	4.5	
	Define read/control/write operations and assign permisions and restrictions accordingly	4.7	
Client	Client informed of remote services	4.1	
	Contractual agreement between service organization and client	4.2	
	Evidence of communication with the client at start and close of control and write functions	4.4	

alia
connecting security interests

Guide Euralarm disponible
Euralarm handboek beschikbaar

CLC/TS 50136-10

Accès à distance

Toegang op afstand

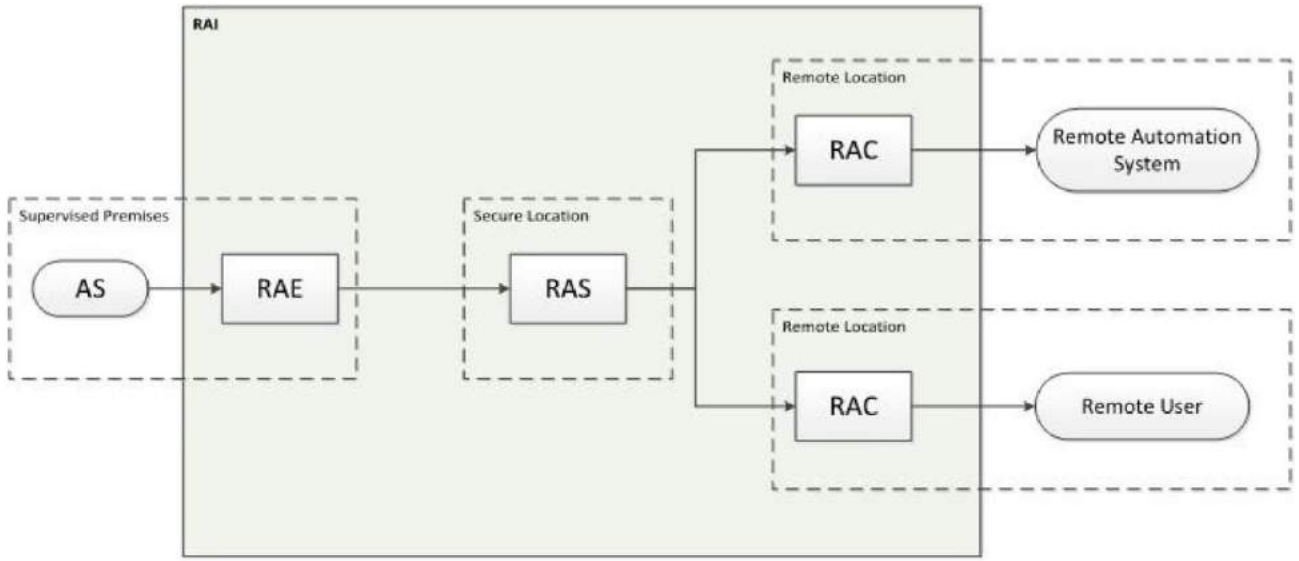


Figure 1 — Remote access infrastructure logical diagram

TS50136-10 CLC TC79 WG5	Alarm systems - Alarm transmission systems and equipment - Part 10: Requirements for remote access.		
	This standard specifies minimum requirements for secure connection and session for remote access to alarm systems. This standard specifies the requirements for the performance, reliability, integrity and security of a Remote Access Infrastructure.		
Functionality	**Requirement**	**Chapter**	**Check**
RAISP	Responsible for security measures to protect the RAI	5	
	Shall apply security measures, described in the technical documentation	5.1	
	Data integrity protection following EN50136-1 6.8.1	5.2	
	Data encryption following EN50136-1 6.8.1	5.2	
	Only authenticated connections allowed from RAE and RAC to RAS	5.3	
	Two factor authentication	5.3	
	Login attempts restricted to limit risk of brute attack	5.3	
	Timeouts after inactivity	5.3	
	Remote user information inside RAI protected	5.3	
	Remote users or third party systems privileges to the RAI management	5.4	
	Monitor and log authenticated user login and logout, authenticated RAE connections, authenticated RAC connections	5.5	
	Monitor and log modifications to RAI configuration by RAISP	5.5	
	Monitor and log modifications of credentials and privileges	5.5	
	Monitor and log security related events	5.5	
	RAI performance criteria and levels agreed. Performance monitoring	6	
	Responsible for documentation (planning, installation, commissioning, service and operation of the RAI)	7.4	
	Responsible for risk management processes (Technology, Continuity Management, Risk Management, Identity Management, Configuration Management, Cyber security)	8	
RAE	It shall be authenticated	5.3	
	No hardware requirements	7.3	
	It shall no affect normal operation/performance of the connected alarm system	7.3	
	Hosted in the supervised premises	7.3	
RAC	It shall be authenticated	5.3	
	No physical requirements	7.1	
	Managed by RAISP	7.1	
RAS	It shall be authenticated	5.3	
	No hardware requirements	7.2	
	Hosted in secure location (alternatively located at the supervised premises)	7.2	
	Managed by RAISP	7.2	
Structure	Additional applications for the RAI shall be arranged so that RAI requirements in this TS are still met	4.1	
	RAI shall be designed to only allow connections between RAE and RAS on one end, and between RAS and RAC on the other end.	4.2	
	Connection between RAC and RAE only allowed via RAS	4.2	

alia
connecting security interests

Guide Euralarm disponible
Euralarm handleiding beschikbaar

Webinaire présentant le guide Euralarm

Webinar over de Euralarm gids

Version anglaise disponible sur YouTube

Engelse versie beschikbaar op YouTube

Version française en préparation

Franse versie in voorbereiding

alia
connecting security interests

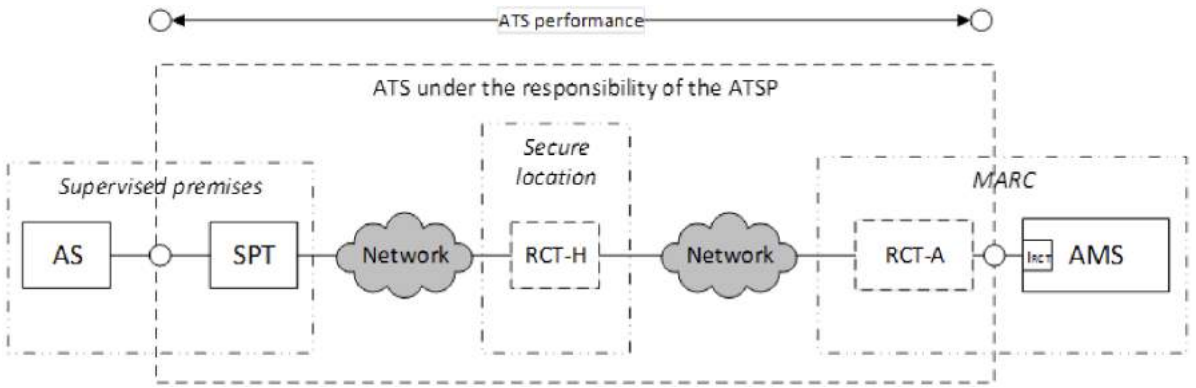
Guide Euralarm en préparation
Euralarm handleiding in voorbereiding

Comment contracter un service cloud en toute sérénité

Met vertrouwen een cloudservice contract afsluiten

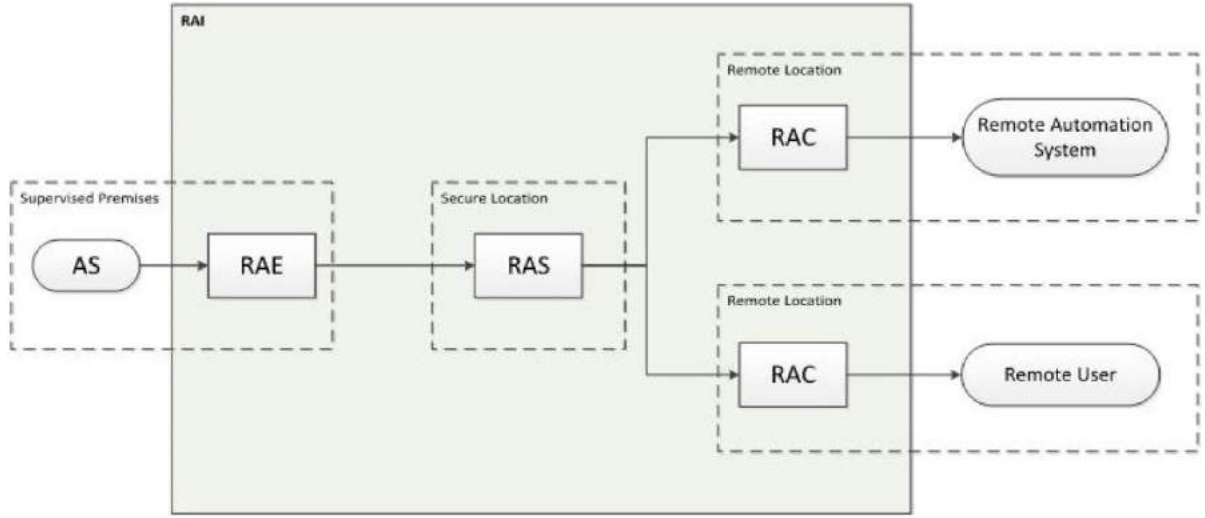
Pour une transmission sûre des alarmes via IP

Voor een veilige verzending van alarmen via IP



Pour un accès à distance sécurisé via le cloud

Voor een veilige toegang op afstand via de cloud



alia
connecting security interests

Guide Euralarm en préparation
Euralarm handleiding in voorbereiding

Projet de contenu

- Types d'implémentation cloud
  Chez le fabricant, à domicile, en data centre, cloud
- Critères légaux pour la localisation des serveurs
- Modèles de cloud
  Data Centre Hosted, IaaS, PaaS, Serverless Computing, SaaS
- Distribution des rôles et responsabilités
  Notamment en matière de cybersécurité
- Normes et schémas de certification
- Recommandations pour les termes du contrat

Inhoud project

- Soorten cloud implementatie
  Bij de leverancier, thuis, in een datacenter, in de cloud
- Wettelijke criteria voor de plaats van servers
- Cloud modellen
  Data Centre Hosted, IaaS, PaaS, Serverless Computing, SaaS
- Toewijzen taakverdeling en verantwoordelijkheden
  Vooral op het gebied van cyberveiligheid
- Normen en certificerings schemas
- Aanbevelingen voor contractvoorwaarden

alia
connecting security interests

Merci pour votre attention
Dank U voor uw aandacht

Benoît Stockbroeckx

Euralarm Technical Manager

euralarm

for a safer and more secure Europe

alia

connecting security interests

alia
connecting security interests

Pauze

Pause

David Gilsoul

Team Inspecties Algemene Directie Veiligheid & Preventie: met U, voor U

Team Inspections de la Direction Générale Sécurité & Prévention: avec vous, pour vous

Team Inspections

Qui sommes-nous?

Quel est notre rôle?

Comment effectuons-nous notre mission et pourquoi ?

alia
connecting security interests

Team Inspections

Qui sommes-nous?

SPF Intérieur

Direction Générale Sécurité et Prévention

Sécurité privée	Inspections	Sanctions
(B. Hoffer)	(D. Gilsoul)	(A. Honhon)

alia
connecting security interests

Team Inspections

Quel est notre rôle?

- Surveillance de la bonne application de la loi du 02/10/2017 réglementant la sécurité privée et particulière et de ses arrêtés d'exécution

1. S'assurer que les restrictions d'accès à la profession soient respectées sur le terrain;
2. S'assurer que les actes posés par les acteurs de ces secteurs respectent les droits essentiels des citoyens tels qu'établis au sein de la réglementation;
3. Renforcer la crédibilité du secteur vis-à-vis des partenaires de la sécurité publique, en s'assurant entre autres de sa bonne organisation administrative.

alia
connecting security interests

Team Inspections

Comment effectuons-nous notre mission et pourquoi?

- Réalisation d'inspections dans le secteur de l'installation de systèmes d'alarmes et de caméras
  - Focus essentiel sur les autorisations (individuelles/entreprises) et les formations ainsi que sur le respect des droits des citoyens (code installateur, matériel utilisé);
  - Focus secondaire sur les autres obligations d'ordre administratif (mentions obligatoires, …);

- Traitement des plaintes
  - Toute plainte est analysée pour déterminer :
    - Si les éléments sont fondés;
    - Si nous sommes bien compétents pour traiter des informations transmises;
    - Le moyen le plus efficace pour mettre fin à l'éventuelle infraction.

- Veille active informations disponibles en open-source;

- Traitement des informations transmises par les services partenaires.

alia
connecting security interests

Team Inspections

Comment effectuons-nous notre mission et pourquoi?

Les plaintes traitées en 2023, en détail :

- 63 plaintes reçues pour les matières relatives à l'installation de systèmes d'alarme et/ou de caméras :
  - Dont 11 relatives à l'obligation de remise d'un code d'installateur :
    - Dans 3 dossiers seulement, la verbalisation a été possible (faits avérés).
  - Dont 21 relatives à des personnes/entreprises non-autorisées :
    - Dans 8 dossiers, verbalisation possible, 8 classements sans suites, 5 dossiers encore ouverts;
    - La simple mention « alarme » sur un véhicule, est un indicateur, mais pas suffisant pour verbaliser (vente est libre).

Les inspections menées en 2023, en détail :

- 98 inspections (contre 112 en 2022) :
  - Dont 35% sans constat d'infraction;
  - Infractions principales : travail sans carte d'identification, entreprise non-autorisée, carte d'identification « périmée » non-renvoyée, absence de la mention de l'autorisation.

alia
connecting security interests

Team Inspections

Comment effectuons-nous notre mission et pourquoi?

Pourquoi effectuons-nous cette mission?

- Focus sur la **sécurité** du citoyen, de la société :
  - Exemple concret d'un concepteur de systèmes d'alarmes, d'un installateur, engagé par une entreprise alors qu'il ne détient pas de carte d'identification;

- Le traitement des plaintes permet de réduire la concurrence déloyale;

➔ Le contrôle effectué sur ce secteur est bénéfique pour tous.

alia
connecting security interests

Team Inspections

Comment effectuons-nous notre mission et pourquoi?

Le Team Inspections avec vous et pour vous car :

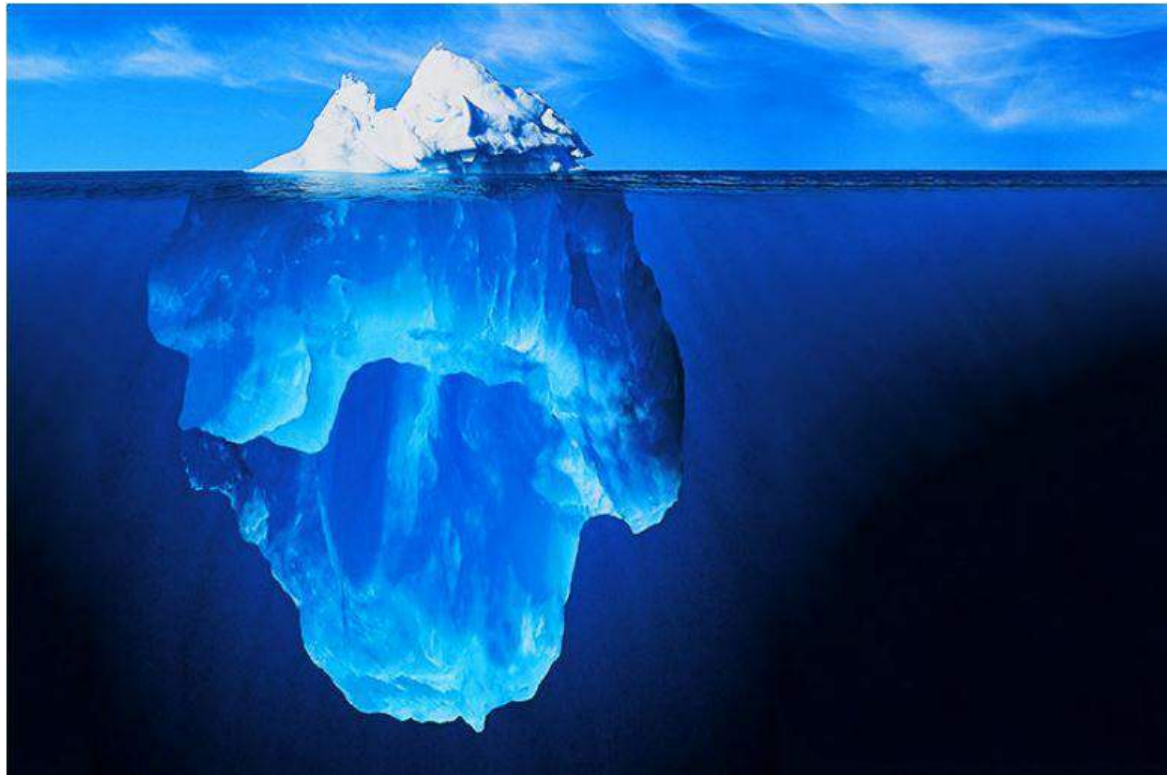
- Nous veillons à lutter contre la concurrence déloyale au sein du secteur, posée par les acteurs non-autorisés;
- En implémentant un cadre réglementaire strict, nous veillons à ce que la réputation de respectabilité des acteurs du secteur soit assurée;
- En établissant cette respectabilité, nous faisons en sorte que vous soyez perçus comme des partenaires fiables pour assurer la sécurité des citoyens, entreprises, institutions.

alia
connecting security interests

Team Inspections

Comment effectuons-nous notre mission et pourquoi?

… et pour assurer au mieux notre mission, nous avons besoin de vous :



Merci pour votre attention!

spvcontrole@ibz.be

https://www.besafe.be/fr/contact/formulaire

Numéro de permanence : 02/488 34 93

alia
connecting security interests

Marita Vranckx

Talent aantrekken: hoe maak jij het verschil?

Attirer les talents : comment faire la différence ?

Marita Vranckx

20 ans d'expérience, 4 jaar als zelfstandige

Agences d'intérim, consultancy, operations management, ressources humaines, general management

Recruitment manager voor grote bedrijven (Bpost, Toyota Motor Europe, Abbvie…)

Support RH pour PME

Recruitment & selection services / headhunting

Ervaring binnen de security sector

alia
connecting security interests

UITDAGINGEN

L’offre et la demande

Le recrutement devient de plus en plus coûteux et exigeant.

Où trouver des candidats ?

Que recherchent les candidats ?

Tout le monde pêche dans le même étang

Grote en kleine(re) bedrijven

Waarom zouden ze voor mij kiezen?

Kiezen kandidaten voor grotere of kleinere bedrijven?

Waar maak ik het verschil?

Hoe competitief zijn

Impact

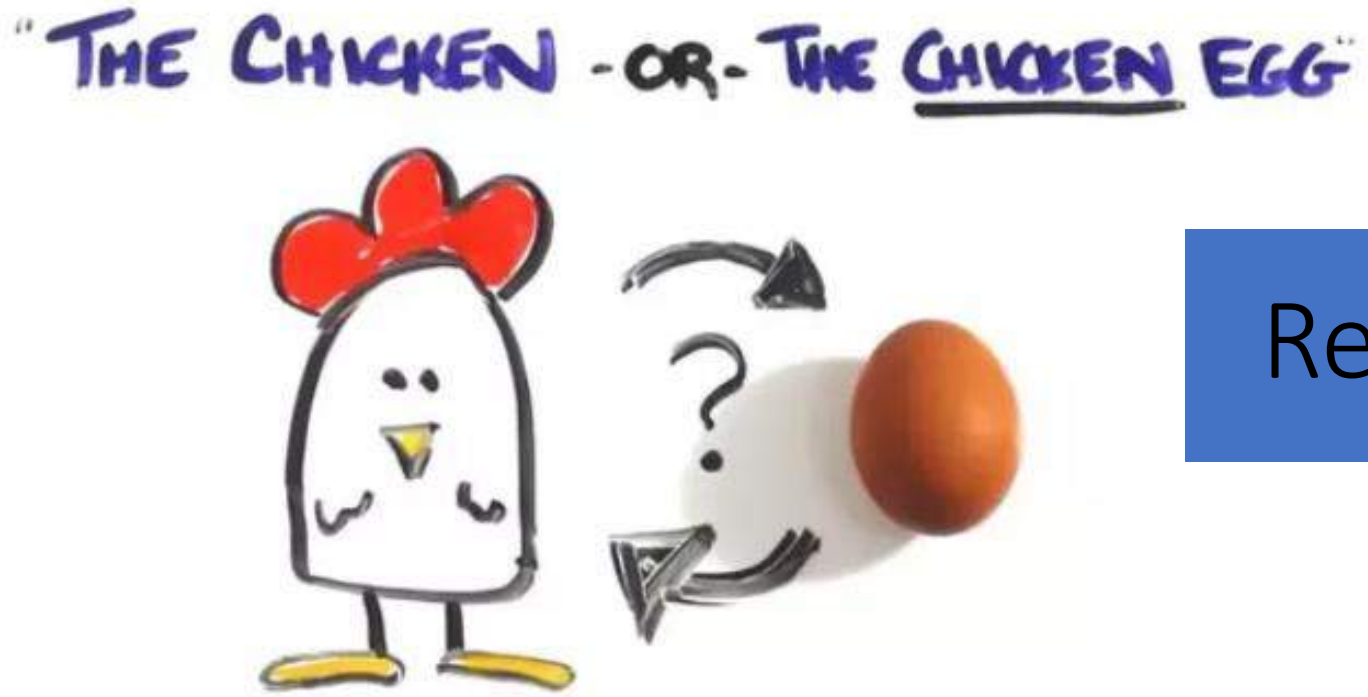
Ik kan mijn klanten niet meer (tijdig) bedienen?

Hoe kan ik nog groeien als bedrijf zonder personeel?

Quel est l'impact d'un "mauvais" recrutement ?

Quel est l'impact d'une rotation importante?

PENURIE DE PERSONNEL



Recrutement

alia
connecting security interests

CANDIDATE JOURNEY

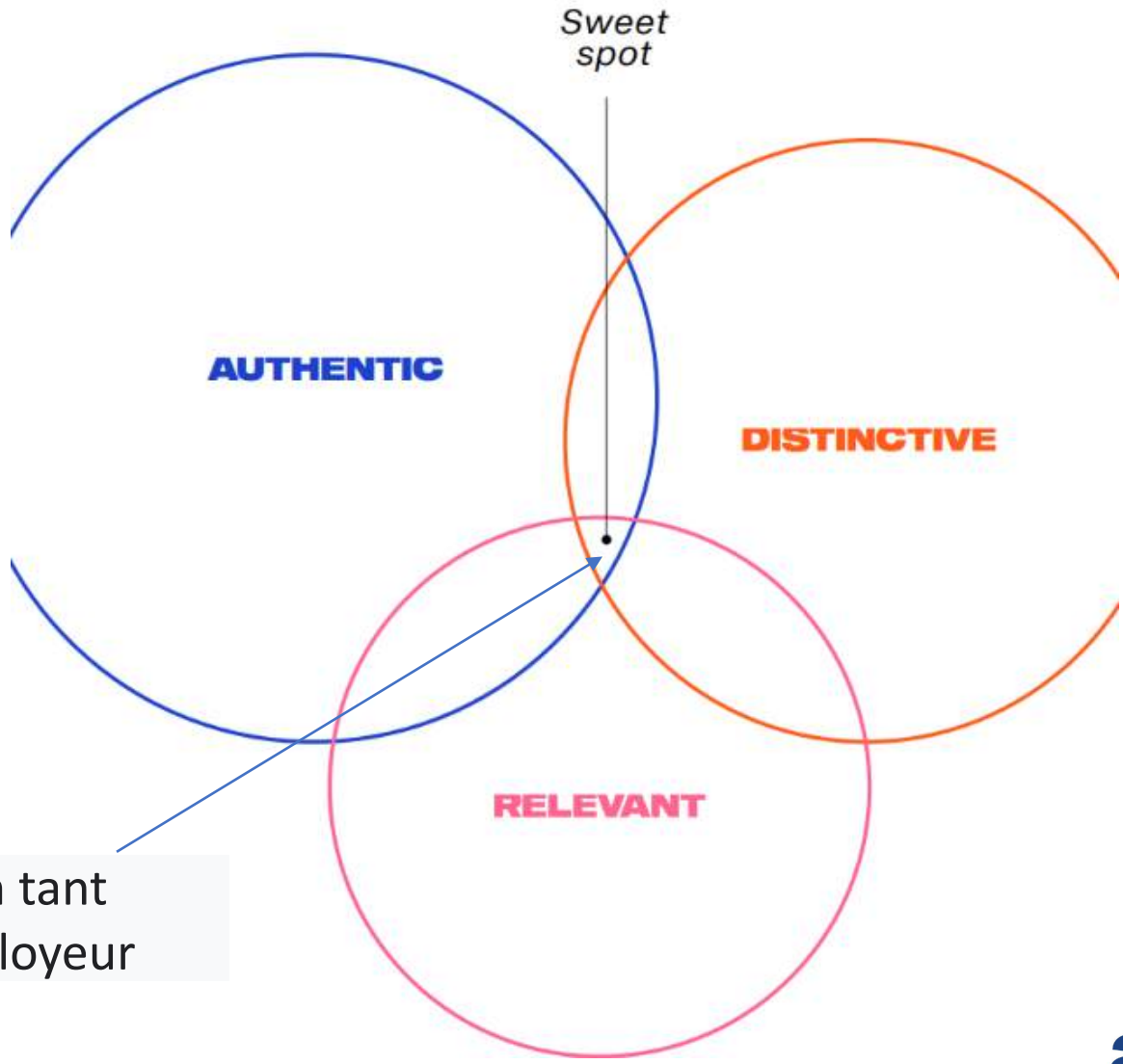
1. Employer brand
2. Aantrekken
3. Compétences
4. Candidate experience
5. Contract
6. Onboarding
7. Rétention

alia
connecting security interests

1. EMPLOYER BRAND : qui êtes-vous en tant qu'employeur ?

Votre image

1. EMPLOYER BRAND : employer value proposition (EVP)



Vous en tant qu'employeur

Màvia BV

1. EMPLOYER BRAND

Wie bepaalt ons imago als werkgever?

- Bedrijfsleiding
- Werknemers
- Familie en vrienden van werknemers
- Ex-werknemers
- Leveranciers
- Concurrenten
- Subco's
- Klanten
- …..

Chaque contact interne et externe peut avoir un impact sur votre réputation.

Zorg dus ook steeds voor een zo positief mogelijke ervaring wanneer je afscheid moet nemen van werknemers.

alia
connecting security interests

Hoe/ waar kandidaten vinden?

2. AANTREKKEN

Vacature:	Titel = max 35 letters om makkelijk leesbaar te zijn op de gsm
	Schrijf een vacatureteksT vanuit het perspectief van de kandidaat
	Zorg dat je een aantal kernwoorden gebruikt die makkelijk te vinden zijn
	Schrijf inclusief / niet té specifiek
	Benadruk een aantal toegevoegde waarden die jij als bedrijf kan bieden
	Kies de juiste plaats om te adverteren op basis van je publiek: VDAB, FOREM Stepstone, Facebook, Tiktok, LinkedIn, Indeed, ….
L'aide extérieure?	Agences de sélection
	Agences d'intérim
	Refer-a-friend
	Visites d'engtreprise / visiter les écoles / stages, …

Competentie gebaseerde screenings / transferrable skills

3. COMPETENCES

- ✓ Les compétences que je recherche sont-elles présentes sur le marché ?
- ✓ Quelles sont les compétences transférables ?
- ✓ Pouvons-nous former les gens nous-mêmes ?
- ✓ Donner la priorité aux connaissances ou à l'attitude ?
- ✓ Acheter des personnes à la concurrence ou former des jeunes

➡ Faire preuve d'ouverture d'esprit sur un marché du travail tendu

<u>Waar vinden we deze mensen?</u>

- ➢ Concullega's
- ➢ School / avondonderwijs
- ➢ Outplacement
- ➢ Vrienden/kennissen/ex-klasgenoten van je werknemers
- ➢ Mensen die al skills hebben die we makkelijk kunnen opleiden om snel inzetbaar te zijn in de security sector => heroriënteren

Professioneel rekruterings-proces

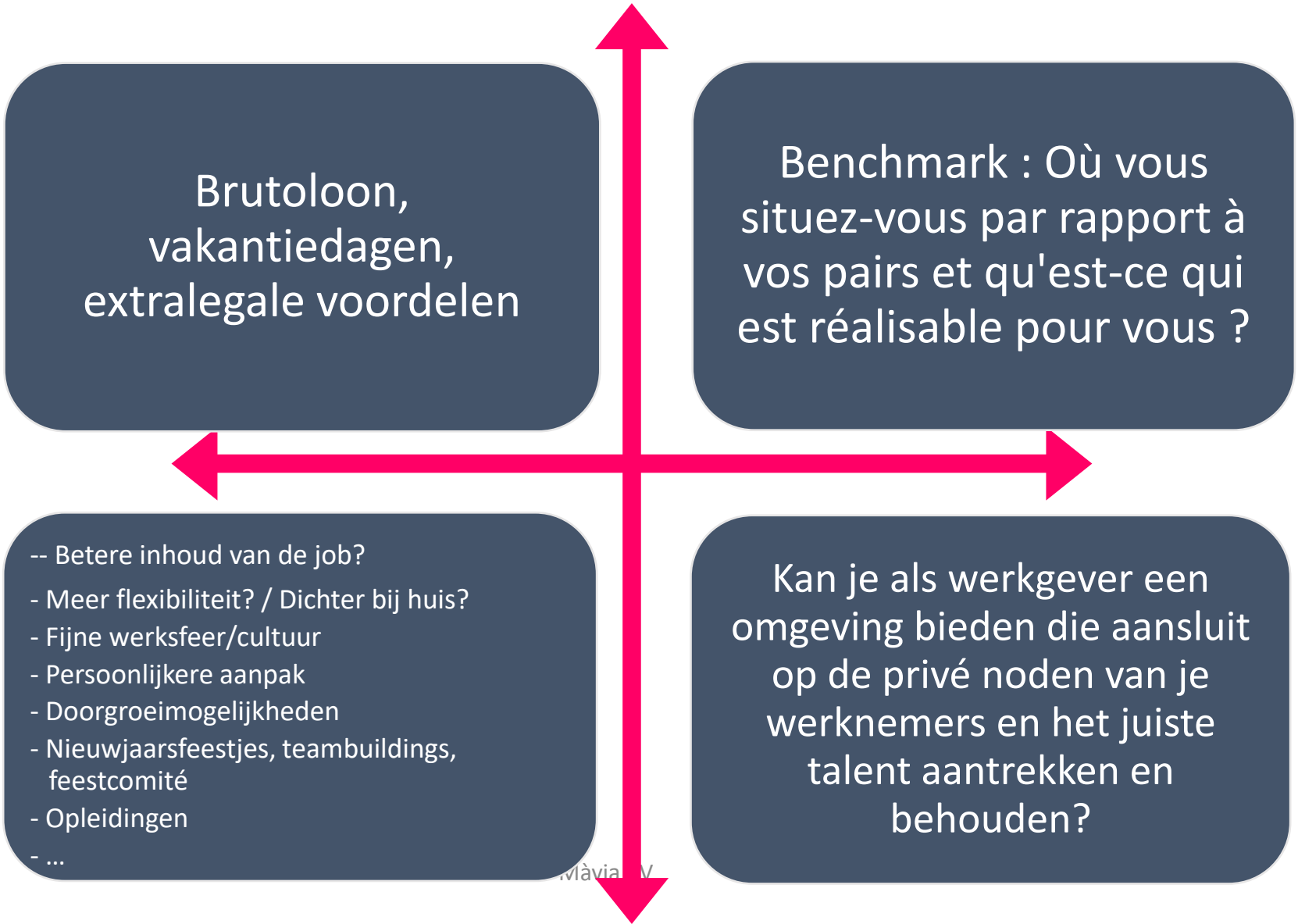
4. CANDIDATE EXPERIENCE

- ✓Wees voorbereid en zorg ervoor dat de kandidaat een duidelijk beeld krijgt van je bedrijf, de open positie en het sollicitatieproces
- ✓Soyez authentique et honnête
- ✓Donnez un retour d'information clair, y compris lorsque vous ne poursuivez pas l'entretien avec le candidat.
- ✓Wees professioneel in het afwijzen van kandidaten, geef elke kandidaat een antwoord. Zij gaan hun netwerk vertellen over zijn/haar ervaring

alia
connecting security interests

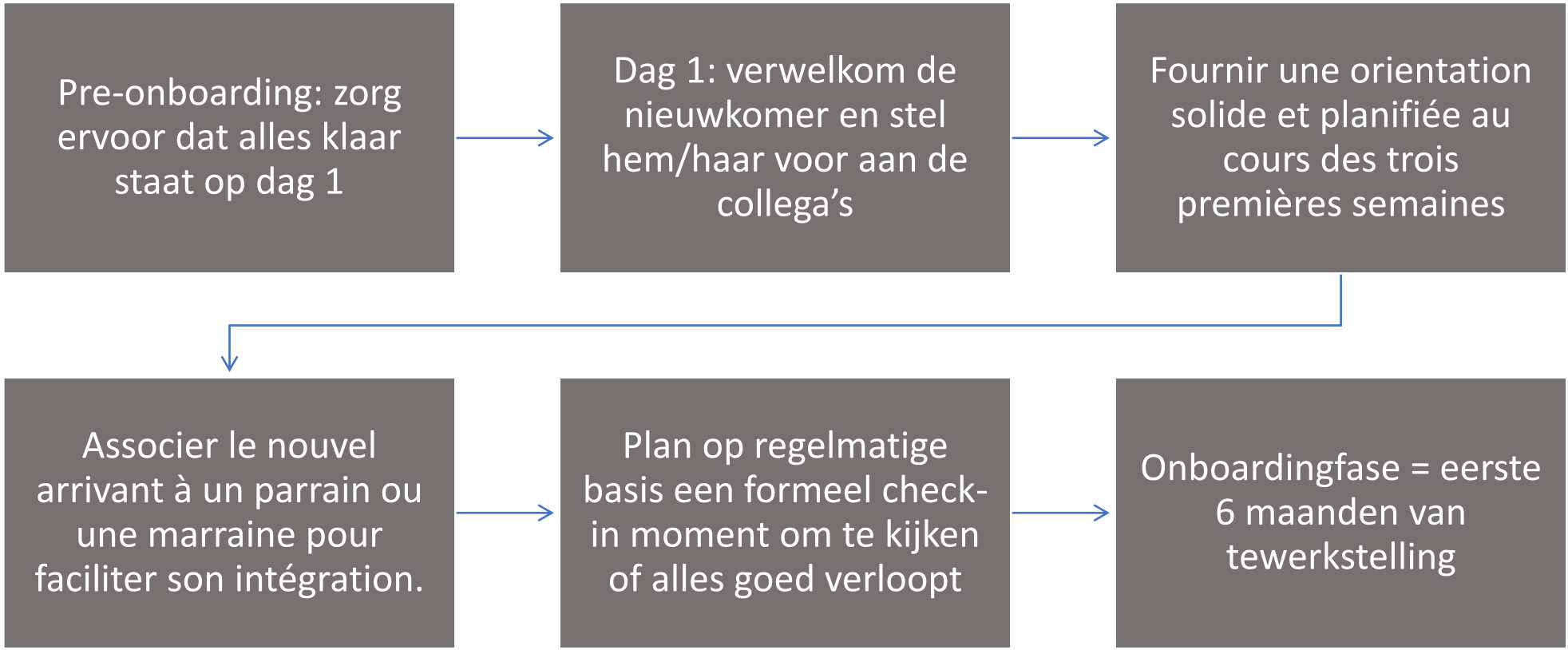
Waar maak jij het verschil?

5. CONTRACT



Onboarding stopt niet na dag 1

6. ONBOARDING



Waarom vertrekken je werknemers?

7. RETENTION

- Salaires et avantages inférieurs aux attentes
- Te hoge werkdruk en/of te weinig steun
- Des possibilités de carrière limitées
- Betere balans tussen werk en privé nodig
- Trop peu de reconnaissance
- Verveling
- Insatisfaits de la direction
- Zorgen over de koers of financiële gezondheid van de onderneming

Tips

7. RETENTIE

Maak oprecht tijd voor ieder individu: luister & probeer het verschil te maken

Créer une culture d'entreprise où la reconnaissance est essentielle

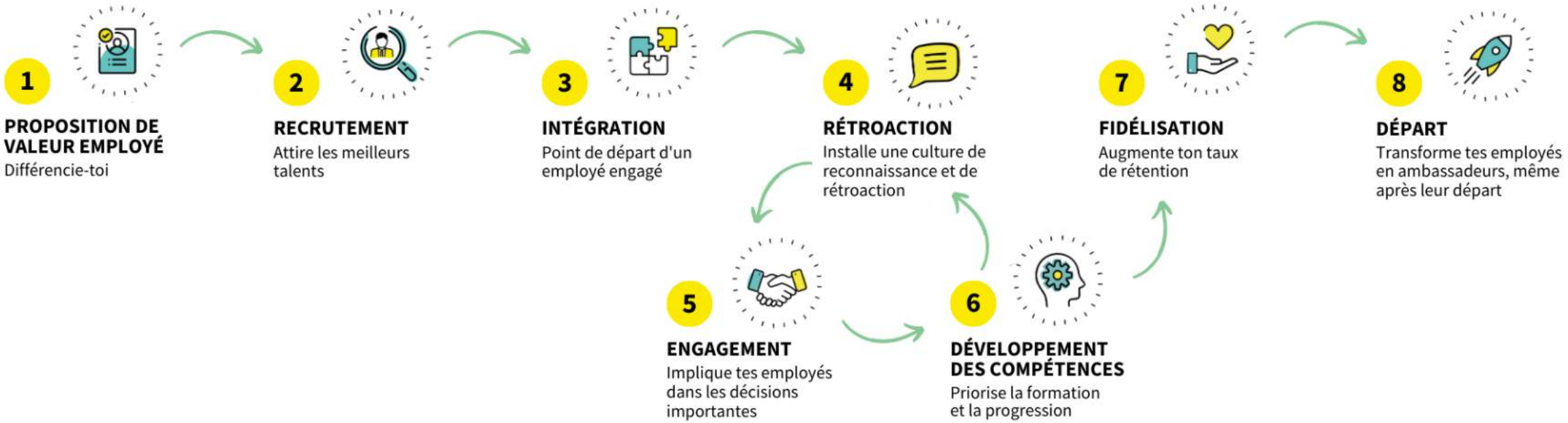
Wees correct en vermijd frustraties door differentiatie in loonpolitiek, behandeling, vriendjespolitiek

Fournir le bon emploi dans le contexte des compétences de vos employés

Geef aan je gevestigde waarden evenveel kansen als aan je nieuwkomers

Maak tijd voor officiële opvolggesprekken en koppel achteraf terug over de besproken onderwerpen en gestelde vragen

8. CONCLUSIONS



8. CONCLUSIES

Plaats jezelf in de schoenen van de kandidaat.

- - -

L'authenticité et un bon leadership peuvent faire la différence.

- - -

Wees open minded en creatief

8. CONCLUSIONS

BEDANKT / MERCI

Marita Vranckx

MÀVIA BV

Marita.vranckx@outlook.com

Emmanuel Taillieu

Cybersecurity: het belang om zich anders te beschermen

Cybersecurity: L'importance de se protéger autrement

CyberSecurity as a Service

Presentation to

ALIA MEMBERS

Introducing the need to secure your company in a different way…

alia
connecting security interests

Why do we need to protect ourselves differently?

Introducing the need to secure your company in a different way…

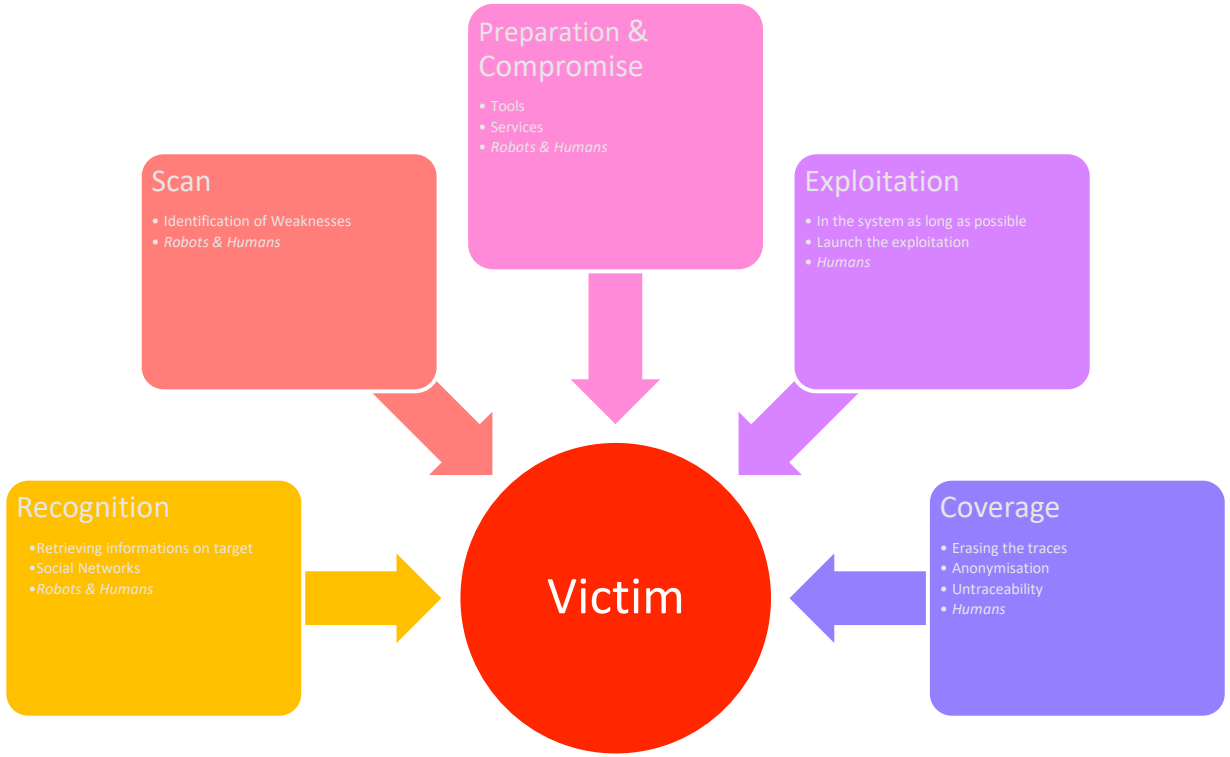
AGENDA

- Introduction
- Threats & Risks
- Situation Today & Challenges
- Another Way
- Benefits of Prevention
- Conclusion

INTRODUCTION

HACKING AS A SERVICE

- Under Continuous Attacks
- Not **If**, But **When**…
- Hacking Steps
- Consequences :
  - Steeling
    and/or
  - Blocking
- 10 Trillions $,
- 20+
- & 279+



TRENDS

THE RISE OF RANSOMWARE ATTACKS

Current trends in cyber security show a marked increase in ransomware attacks in recent years.

THE GROWING THREAT OF ATTACKS TARGETING THE INTERNET OF THINGS (IOT)

Vulnerabilities in IoT devices, which are often less secure, provide cybercriminals with new targets. The risks to businesses and users are high, ranging from identity theft to data loss.

THE RISE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY/CYBERCRIME

Artificial intelligence is playing an increasing role in cyber security, strengthening defences against cyber attacks by predicting and detecting threats. However, AI can also be used maliciously by cybercriminals, resulting in more sophisticated attacks that are harder to counter. This dual reality underlines the importance of developing robust and resilient AI to anticipate these new forms of cybercrime.

THE CHALLENGES OF PROTECTING PERSONAL DATA

Faced with constantly changing regulations, businesses and consumers need to be vigilant. (GDPR, NIS2.0,...)

CYBERSECURITY IN THE CONTEXT OF REMOTE WORKING

Remote working poses specific cybersecurity challenges, with home networks often less secure. Adopting best practice to secure remote infrastructures is crucial,

THE EMERGENCE OF ZERO-DAY THREATS

Zero-day vulnerabilities are unknown security holes that are exploited by hackers before they are discovered by the developer. In the face of these threats, speed of response is crucial, but it is virtually impossible.

RISKS BY SECTORS - EXAMPLES

Police

- Interruption of communication systems
- Loss or alteration of sensitive data
- Attacks on video surveillance
- Falsification of online information

Fire Service

- Attacks on warning and communication systems
- Falsification of fire data
- Attacks on operations management systems

Security

- Compromise of security systems
- Attacks on customer databases
- Sabotage of alarm systems
- IoT-related risks

Common Risks to all three Sectors :

- Ransomware
- Targeted phishing
- Denial of service attacks (DDoS)
- Zero Days
- Insider Threats
- Increased Chinese Attacks

THE SITUATION TODAY

HACKED COMPANIES :

Barreau de Charleroi,
C.P.A.S. de Charleroi,
ChWaPi, André Renard, Vivalia, Tielt,
Herentals,
Gent Haven, Antwerpen Crematorium, ...
Picanol,
Politie Zwijndrecht,
Thales,
Ville de Liège, Stad Antwerpen,
Touring,
...

CONSEQUENCES :

- Operational Impact:
  - Disruption to emergency services
  - Business interruption
- Data Security Impact:
  - Compromise of sensitive data
  - Loss of data
  - Breach of confidentiality
  - Loss of trade secrets
- Impact:
  - Financial costs
  - Compliance costs
- Reputation and Trust:
  - Loss of trust
  - Reputational damage
- Legal Consequences:
  - Legal liability
- Security Risks:
  - Potential for new attacks
- Human Impact:
  - Stress and employee morale

CHALLENGES

Source : Best Practices reported by Centre for Cybersecurity Belgium

&

RISK = #THREATS X #WEAKNESSES X #ASSETS

FIGURES :

- **55%** of experts report an increase in their **stress** levels due to the intensification of threats...(CFO).
- Large companies were the most affected by cyber-extortion **(40%)**, followed by small organisations **(25%)** and medium-sized companies **(23%)** (Orange Cyberdefense).
- Internal actors, whether deliberate or accidental, were responsible for **37.45%** of detected incidents (OCD)
- Europe saw **85%** of the hacktivist attacks observed in 2023, followed by North America (**7%**) and the Middle East (**3%**) (OCD).
- Small organisations (1 to 250 employees) have the **highest rate** of targeted malicious emails (Comparitech).
- In a recent Gartner survey, **80%** of organisations said they planned to increase their spending on information security in 2024. (Gartner).

LACK OF :

- Competences,
- Budget,
- Time

CYBERATTACKS REQUIRES EMERGENCY RESPONSE ... IN ADDITION TO TRADITIONAL APPROACH.

TRADITIONAL APPROACH

"THE TRADITIONAL APPROACH FAILS TO PROVIDE CLEAR VISIBILITY INTO INCIDENTS AND WEAKNESSES."

BACKUP, YES… BUT NO !

USUAL IT SERVICES & SECURITY PRODUCTS

- Firewalls, XDR, IDP, SOC, SIEM, Security Assessments, …
- **Traditional Approach =** Necessary but NOT sufficient :
  - Vulnerabilities inherent in traditional security products : Lack of regular updates, Weak communication protocols, weak authentication, etc.
  - Challenges associated with updating these systems: Cost and complexity of updating, compatibility, dependence on third-party suppliers, hardware limitations, reluctance to change, etc.

FACING EVOLUTION OF CYBER THREATS

- Ransomware Attacks, Phishing and Social Engineering, Data Breaches (steeling), Internet of Things (IoT), Cloud Security Challenges, Supply Chain Attacks (compromising legitime software), Zero-day Vulnerabilities, …

HACKING EMERGENCY RESPONSE

…MUST BE EMPOWERED WITH AI, ROBOTS, AND COMMUNITY COLLABORATION

HUMAN LIMITATIONS:

Humans are facing challenges in high-pressure hacking incidents, including stress-induced errors.

SWIFT AND PRECISE ACTION:

Immediate and accurate responses are needed during hacking emergencies to minimize damage.

AI AND ROBOT EFFICIENCY:

AI and robots excel in emergency response, processing data rapidly without succumbing to human limitations.

ERROR REDUCTION:

AI has a role in reducing errors by operating on predefined algorithms and without the influence of stress.

MUTUALISATION AND COMMUNITY COLLABORATION:

Mutualisation and community collaboration are powerful, where AI technologies share insights and responses, enhancing the collective strength of the cybersecurity community.

OUR VISION

NO SECURITY = NO BUSINESS

AN APPROACH TO SERENITY

Another Way for Protecting Organisations Against Cybercrime

- Predictive AI Model
- Clear & Concise Cyber Risk Assessment : Evolution of Threats
- Protection vs Hacking (Importance vs Emergency)
- Immediate Protection : Immediate Response to Attacks 365x7x24
- Permanent Realtime Risk Mitigation : Permanent Audit of Security Position
- Continuous Weaknesses Diagnostic
- Regulatory Compliance

BENEFITS OF PREVENTION

FIGURES : 1% VS 20%

PROTECTION OF COMPANY REPUTATION

BUSINESS CONTINUITY

GOVERNANCE

CONCLUSION

CYBERSECURITY IS CRUCIAL FOR ORGANIZATIONS FOR ENSURING PUBLIC CONFIDENCE AND THE PROVISION OF EFFICIENT SERVICES

PREDICTIVE AI MODEL

IMMEDIATE PROTECTION

REALTIME RISK MITIGATION

WEAKNESSES DIAGNOSTIC

A WINDOW ON THE UNKNOWN

alia
connecting security interests

Questions ?

Thank YOU !

alia
connecting security interests

Amadine Vanscheeuwijck

Onderzoek naar het samenwerkingsbeleid tussen publieke en private veiligheidsactoren bij inbraakalarmsystemen

Recherche sur les politiques de coopération entre les acteurs des services publics de la sécurité privée dans les systèmes d'alarme

UNIVERSITEIT
GENT

alia
connecting security interests

FACULTEIT
RECHT EN CRIMINOLOGIE

VAKGROEP CRIMINOLOGIE, STRAFRECHT EN SOCIAAL RECHT
INSTITUTE FOR INTERNATIONAL RESEARCH ON CRIMINAL POLICY

ONDERZOEK NAAR

HET SAMENWERKINGSBELEID TUSSEN PUBLIEKE EN PRIVATE

VEILIGHEIDSACTOREN BIJ INBRAAKALARMSYSTEMEN

ALIA Security Day 28 maart 2024 Drs. Amandine Vanscheeuwijck

UNIVERSITEIT
GENT

alia
connecting security interests

CONTENU

1. Conception de la recherche
2. Méthodologie
3. Processus
4. Bibliographie

UNIVERSITEIT GENT

alia
connecting security interests

ONDERZOEKSOPZET

UNIVERSITEIT GENT

alia
connecting security interests

ONDERZOEKSOPZET

Zomer 2022: bestek ADVP

1. In kaart brengen van de actuele situatie
   - A. Lokaal niveau
     - i. PZ's
     - ii. Gemeentes
     - iii. Sanctieprocedure
   - B. Federaal niveau
     - i. 101- en 112-centrales
     - ii. CIC's
   - C. Niveau van de sector van private bewakingsondernemingen
   - D. Niveau van de alarmgebruiker
2. Vaststellen van de sterktes en knelpunten bij elke actor
3. Formuleren van praktische en beleidsaanbevelingen

Promotorschap : Prof. Dr. Pieter Leloup (Universiteit Gent – Vrije Universiteit Brussel)
Prof. Dr. Marc Cools (Universiteit Gent)

UNIVERSITEIT GENT

alia
connecting security interests

MÉTHODOLOGIE

UNIVERSITEIT GENT

alia
connecting security interests

MÉTHODOLOGIE

1. Analyse de la littérature

A. Phénoménologie
B. Développement du cadre réglementaire

2. Analyse juridique

A. Loi du 2 octobre 2017
B. AR du 25 avril 2007
C. AM du 8 mars 2010

3. Analyse qualitative

A. Analyse 96 pvs DGSP
B. 19 entretiens; 29 répondants
C. 5 groupes de discussion; 13 participants

4. Analyse quantitative

A. Police locale; police fédérale
B. ALIA Security; Association des Centres d'Alarmes
C. Enquête utilisation des systèmes d'alarmes

5. Analyse de la politique (Patton, Sawicki & Clark, 2015)

UNIVERSITEIT GENT

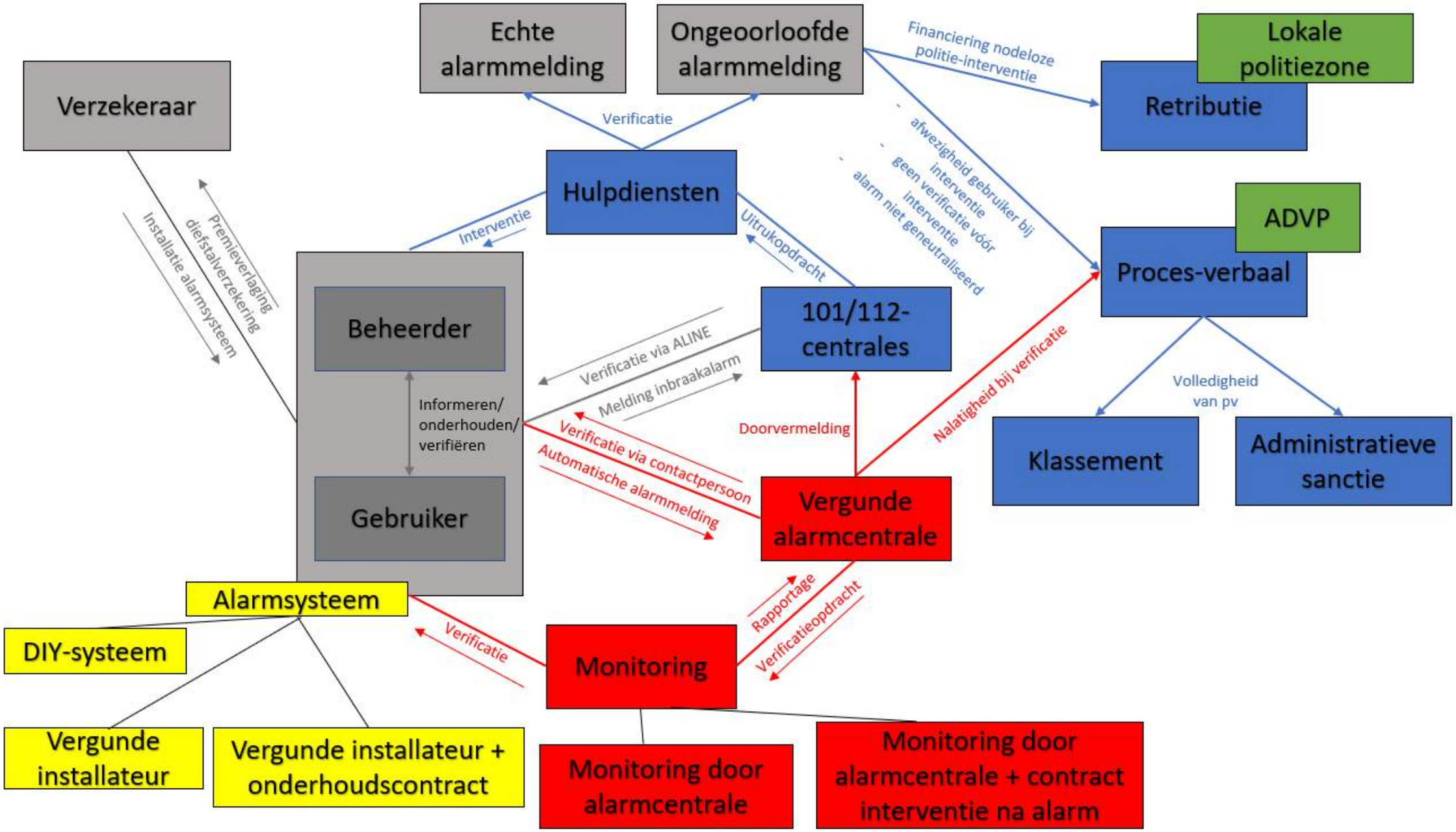
alia
connecting security interests

PROCES

UNIVERSITEIT GENT

alia
connecting security interests

PROCES


Echte alarmmelding
Ongeoorloofde alarmmelding
Financiering nodeloze politie-interventie
Lokale politiezone
Retributie
Verzekeraar
Verificatie
Hulpdiensten
- afwezigheid gebruiker bij interventie
- geen verificatie vóór interventie
- alarm niet geneutraliseerd
ADVP
Proces-verbaal
Interventie
Uitrukopdracht
Premieverlaging diefstalverzekering
Installatie alarmsysteem
Beheerder
101/112-centrales
Verificatie via ALINE
Melding inbraakalarm
Informeren/ onderhouden/ verifiëren
Gebruiker
Doorvermelding
Nalatigheid bij verificatie
Volledigheid van pv
Klassement
Administratieve sanctie
Verificatie via contactpersoon
Automatische alarmmelding
Vergunde alarmcentrale
Alarmsysteem
Rapportage
Verificatieopdracht
Verificatie
DIY-systeem
Monitoring
Vergunde installateur
Vergunde installateur + onderhoudscontract
Monitoring door alarmcentrale
Monitoring door alarmcentrale + contract interventie na alarm

BIBLIOGRAFIE

UNIVERSITEIT GENT

alia
connecting security interests

BIBLIOGRAFIE

Beleidsanalyse

Patton, C., Sawicki, D., & Clark, J. (2015). *Basic Methods of Policy Analysis and Planning* (3de dr?). Routlegde.

Onderzoeksrapport

Vanscheeuwijck, A., Van der Hoeven, E., Leloup, P., & Cools, M. (expected 2024). *Onderzoek naar de sterktes en knelpunten in het samenwerkingsbeleid tussen publieke en private veiligheidsactoren bij de installatie, het onderhoud en het gebruik van inbraakalarmsystemen en het beheer van alarmcentrales*. (p. 199). Algemene Directie Veiligheid en Preventie, Federale Overheidsdienst Binnenlandse Zaken.

FACULTEIT
RECHT EN CRIMINOLOGIE

Drs. Amandine Vanscheeuwijck

PhD researcher

INSTITUTE FOR INTERNATIONAL RESEARCH ON CRIMINAL POLICY

VAKGROEP CRIMINOLOGIE, STRAFRECHT EN SOCIAAL RECHT

E Amandine.Vanscheeuwijck@UGent.be

M +32 479 53 73 01

www.ugent.be

Universiteit Gent

@ugent

@ugent

Ghent University

UNIVERSITEIT
GENT

alia
connecting security interests

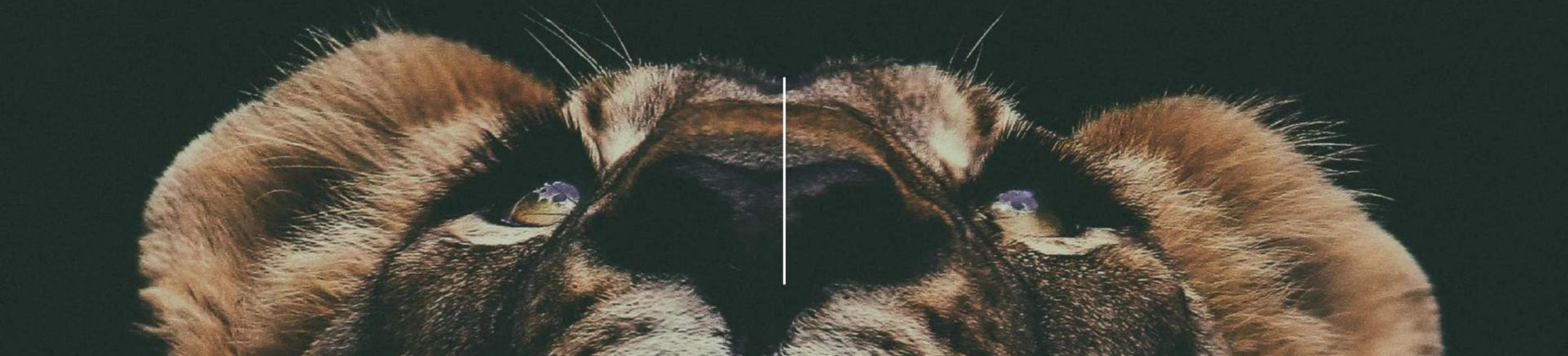
Matthias Dobbelaere

AI, Cybercriminaliteit en privacy

L'IA, la cybercriminalité et la vie privée


IS
PRIVACY
‘BORING’?
MISSCHIEN WEL.

... EN WIE BEGLUURT ONS?



TOPICS

ELON — PRIVACY — SURVEILL

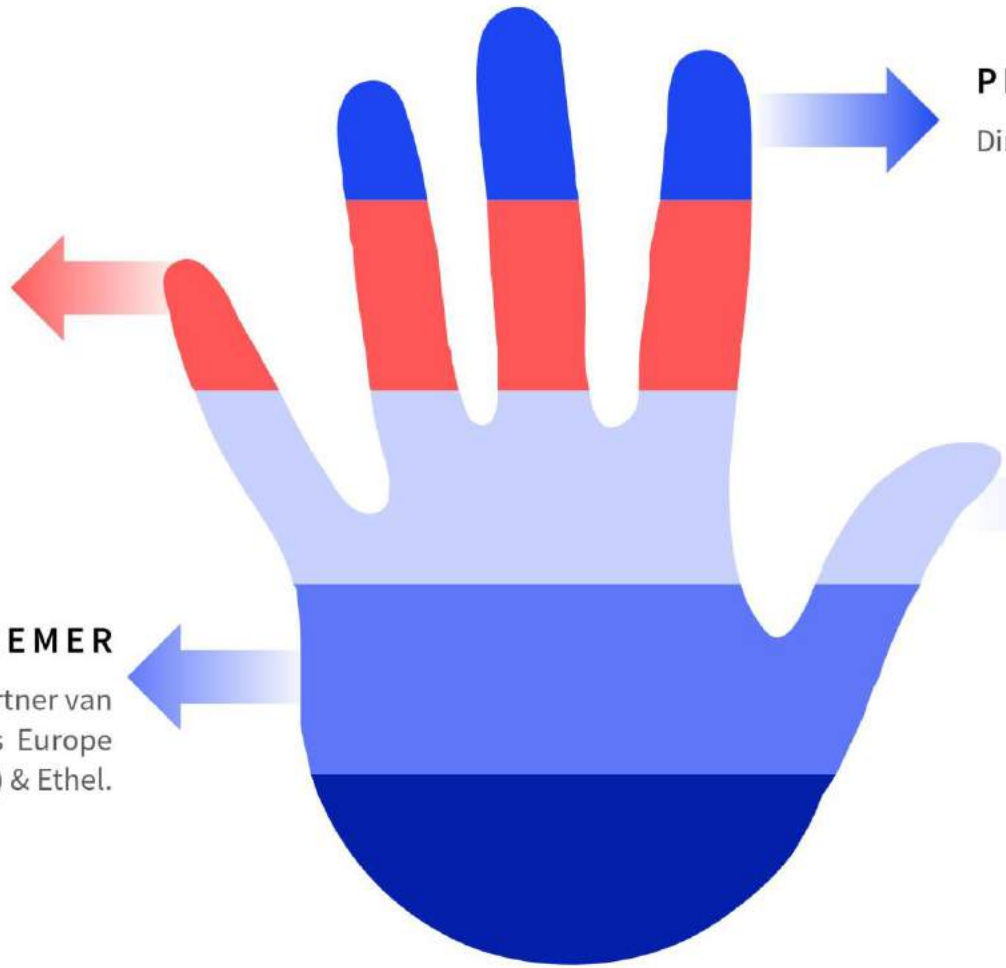
ANCE — BIOMETRIE — GDPR —

AI — CAMERAWET — CHATGPT

WIE IS
DIENEN VENT?

MATTHIAS DOBBELAERE-WELVAERT

@DOBBELAEREW



PRIVACYJURIST/-ACTIVIST

Directeur 'Ministry of Privacy'

DOCENT

Erasmus Hogeschool Brussel

AUTEUR

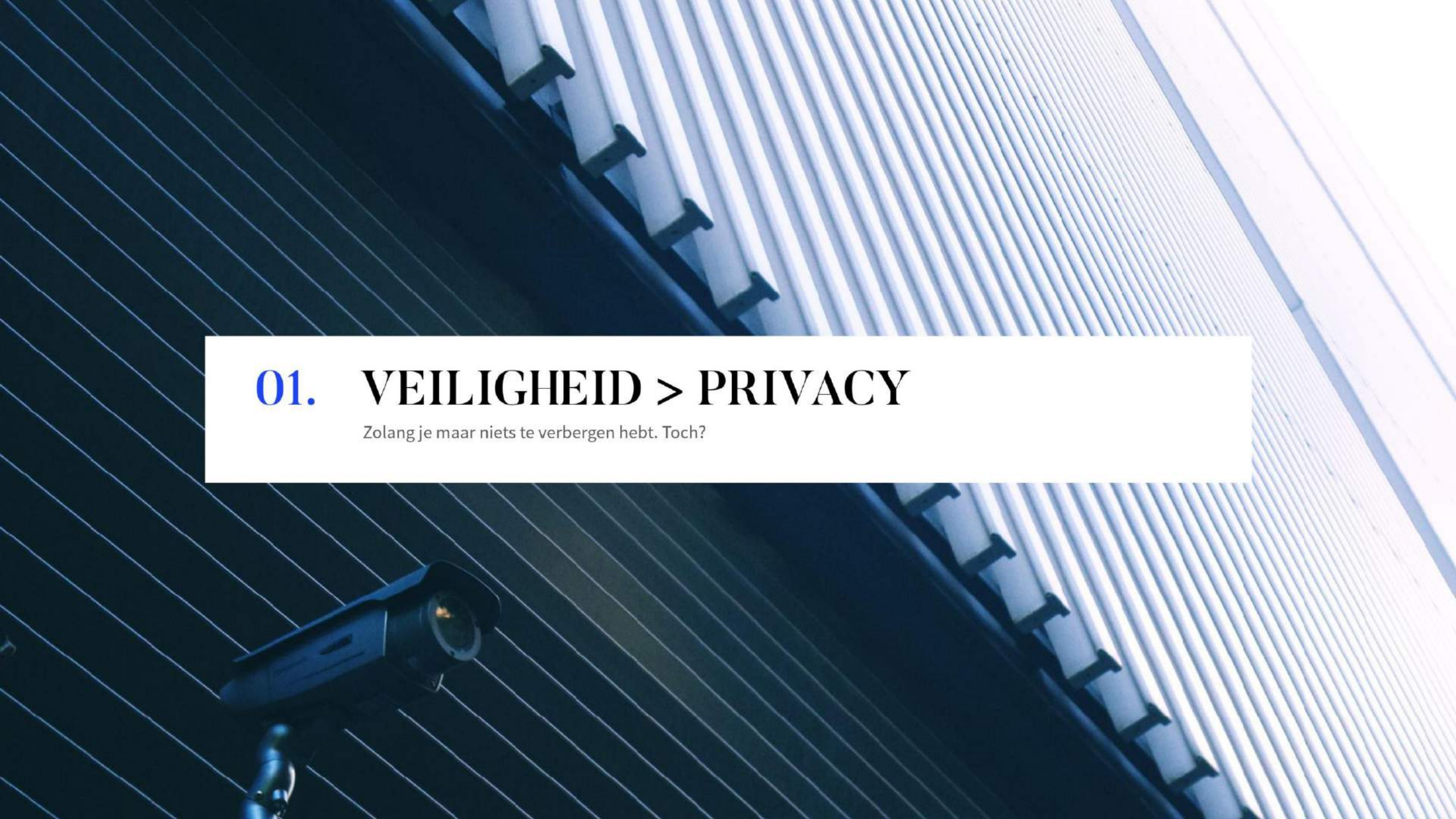
'Ik weet wie je bent en wat je doet'

ONDERNEMER

Oprichter en ex-partner van theJurists Europe (deJuristen) & Ethel.


DOE EVEN JE OGEN TOE.


WAT LEERT ONS DIT
INGEBORG-MOMENT?



01. VEILIGHEID > PRIVACY

Zolang je maar niets te verbergen hebt. Toch?

2016

AANSLAG

EN WAT ALS IK HETZELFDE VRAAG MET DEZE FOTO's?

Mensen zijn emotionele wezens. Aanslagen doen ons collectief beseffen dat we toch niet zo veilig zijn als we dachten. Terrorisme is moeilijk te vatten, hoewel de doden uit aanslagen in aantal niet te vergelijken zijn met verkeers- of tabaksdoden, lijkt het gevaar zo significant groot dat we bereid zijn (inclusief onze beleidsmakers) om grote opofferingen in vrijheden te maken. Een begrijpelijke, maar foute reflex.

2021

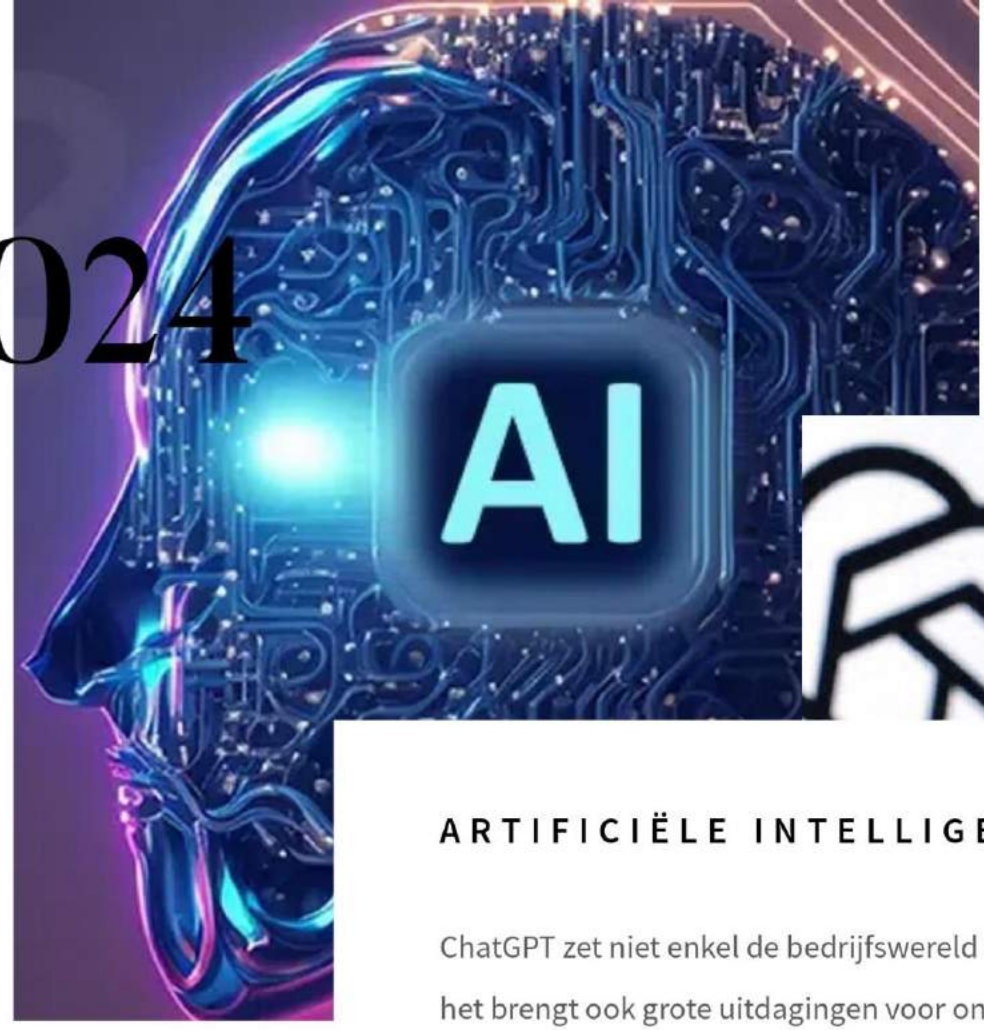
CORONA

Politie

COVID

2020-2021 werd hét tijdperk van de surveillance. Camera's aan de kust, drones boven ons hoofd, warmtecamera's die stoute campingbewoners moesten opsporen, en natuurlijk: ANPR-camera's die plots werden ingezet om de corona-maatregelen te controleren.

2024



ARTIFICIËLE INTELLIGENTIE

ChatGPT zet niet enkel de bedrijfswereld op zijn kop, het brengt ook grote uitdagingen voor onze privacy met zich mee. In de eerste versies kon je makkelijk informatie opvragen over personen: ChatGPT en anderen schuimen immers (online) bronnen af, en maken ze beschikbaar voor hun gebruikers. In Italië werd ChatGPT zelfs even verboden.

AANSLAG

EEN BEETJE GESCHIEDENIS

“PRIVACY MAY ACTUALLY BE AN ANOMALY”
~ VINTON CERF,
CO-CREATOR OF THE EARLY INTERNET PROTOTYPE AND GOOGLE EXECUTIVE.

Privacy, zoals het nu wordt omschreven, is slechts 150 jaar oud. De meeste mensen die door de geschiedenis heen leefden, konden maar weinig op privacy rekenen in hun kleine gemeenschappen. Mensen kiezen steevast voor geld, prestige of gemak, wanneer dit in strijd is met een verlangen naar afzondering.

WAT IS DE TOEKOMST VAN PRIVACY?

ZAL PRIVACY OPNIEUW VERDWIJNEN?

Zal privacy vervagen? De meeste mensen lijken perfect bereid om privacy in te ruilen voor veiligheid, gezondheid (denk maar COVID-19) of eenvoudig gemak. Sommigen zeggen zelfs dat de kosten van privacy te hoog zijn, of spreken in 2024 zelfs van een heuse “privacylobby”.

Drugscommissaris Van Wymersch roept de politiek op om privacywetgeving te versoepelen: "Huidige wetgeving houdt anonimiteit van criminelen in stand"

Nationaal Drugscommissaris Ine Van Wymersch heeft de politici in het parlement opgeroepen om de privacywetgeving te versoepelen. De strenge regels staan een goede aanpak van drugscriminaliteit in de weg, zegt ze. De versoepeling is onderdeel van een breder plan dat Van Wymersch presenteerde om de drugscriminaliteit aan te pakken.

Cisse Michiels

di 19 mrt 19:26

DE VRAAG

KAN HET ONS WAT SCHELEN?

Alle gedane investeringen, geïmplementeerde processen, opleidingen, maar kan het ons eigenlijk wat schelen? Stel jezelf de vraag: hoeveel dataverzoeken heb je sinds 25 mei 2018 verstuurd (of ontvangen)? Hoeveel gegevensverwijderingen? En is een gebrek aan interesse de oorzaak, of een gebrek aan kennis?

Bevraging: Hoe denken Vlamingen over de dataficatie van het publieke domein?

Wereldwijd maken overheden gebruik van ANPR-camera's die auto's flitsen, sensoren die geluidsoverlast meten, bodycams en andere datagedreven technologieën. Ook in Vlaanderen is deze 'dataficatie van de openbare ruimte' een feit. Maar hoe denkt de burger hierover? Dat is het onderwerp van deze studie van het Kenniscentrum Data & Maatschappij.

Elk jaar voert het Kenniscentrum Data & Maatschappij een onderzoek uit waarbij het via een grootschalige bevraging de attitudes, percepties en praktijken van Vlamingen over datagedreven technologieën bevraagt. Dit jaar keek het naar het gebruik van deze technologieën in het publieke domein. Deze technologieën worden vaak geïntroduceerd met als doel de veiligheid te verhogen en diensten te optimaliseren. Maar gebruikersonderzoek over het gebruik van deze technologie blijft schaars. Daar brengt dit onderzoek verandering in.

Dit rapport geeft meer inzicht in:

Enkele **kernbevindingen** uit het rapport**:**

- **ANPR-camera's**, **bodycams** en **vaste camera's** zijn **goed gekend** onder de Vlaming. 84,8% geeft aan dat ze al gehoord hebben van deze technologieën. Andere data-gedreven technologie zoals optische sensoren en audiosensoren zijn minder gekend.

- Ondanks de relatief hoge kennis van data-gedreven technologieën die aanwezig zijn in de openbare ruimte, bestaat er nog **veel onduidelijkheid over de data die deze technologieën verzamelen**.

- Over het algemeen vinden Vlamingen de aanwezigheid van **bodycams** en **vaste camera's aanvaardbaar**. Zo geven respondenten gemiddeld een aanvaardbaarheidsscore van 4.1 op 5 voor bodycams, en 4.2 op 5 voor vaste camera's.

- De **doelstelling** van een technologie heeft een grote invloed op hoe aanvaardbaar die technologie wordt bevonden. 1 op 5 vindt het bijvoorbeeld onacceptabel dat een ANPR-camera wordt gebruikt om sluipverkeer te weren.

- Er heerst een **matige privacybezorgdheid** over de verschillende data-gedreven technologieën. Toch geeft 9 op de 10 Vlamingen aan dat ze veel belang hechten aan de bescherming van hun persoonlijke data.

WAT IS PRIVACY?

MEER DAN EEN MENSENRECHT

Privacy is een mensenrecht, zoals vastgelegd in artikel 8 EVRM. Het recht is echter niet absoluut, beperkingen zijn mogelijk. Overheden kunnen - om de veiligheid van haar burgers te garanderen - beperkingen stellen. Ook privé-bedrijven mogen persoonsgegevens verwerken wanneer je daar zelf toestemming voor geeft, of wanneer zij daar een ‘gerechtvaardigd’ belang bij hebben.

02. CAMERAWET: EEN OPFRISSING

WAT MAG MEN NOOIT FILMEN?

Een private bewakingscamera mag in principe **nooit** de openbare weg filmen. Meer en meer wordt dit in de praktijk onmogelijk, door slimme deurbellen of andere flexibele apparatuur. De wet is echter helder: het mag *niet*.

WPA & CAMERAWET

VERSCHIL WPA & CAMERAWET

WPA: van toepassing op politionele en bestuurlijke camera’s (artikelen 25/1 tot en met 25/8 regelen het zichtbaar gebruik van camera’s, de artikelen 46/2 tot met 46/14 regelen het niet-zichtbaar (dus 'heimelijk') gebruik van camera’s).

CAMERAWET

2018, NIET 2007

De Camerawet werd in 2018 ingrijpend gewijzigd (we zien nog teveel vermeldingen van de Wet van 2007 opduiken). De belangrijkste verplichting die is opgenomen is het **registreren van élke bewakingscamera, geplaatst door particulieren én bedrijven (**enige uitzondering: binnenzijde privéwoning) via aangiftecamera.be

Er dient ook een **register van de beeldverwerking** te worden bijgehouden, én een - juridisch correct - **pictogram (mét vermelding DPO)** te worden geplaatst.

DRONES & DASHCAMS

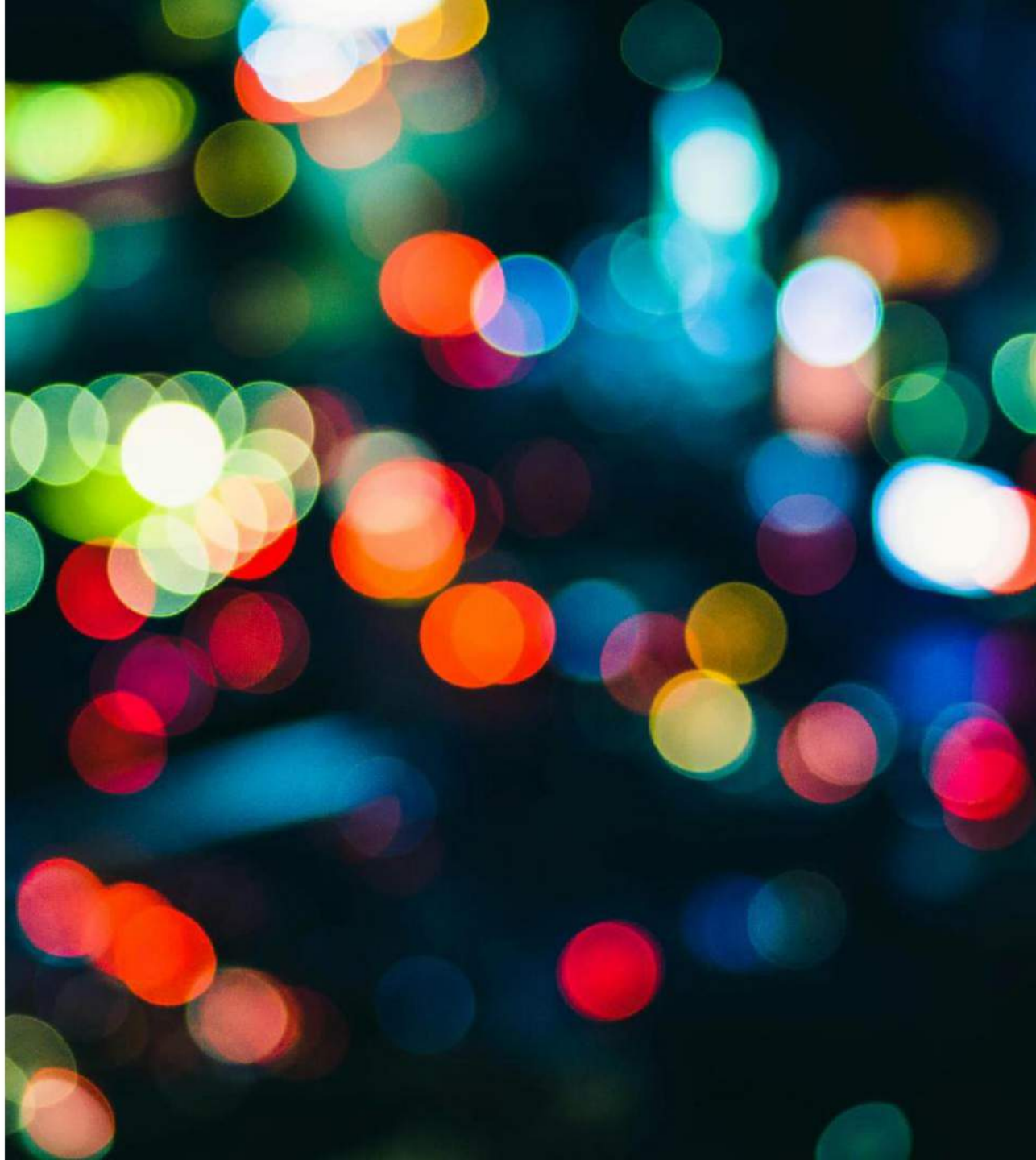
De Camerawet van 2018 - door de GDPR volledig weggecijferd - regelt wel méér dan alleen bewakingscamera's. Ze regelt ook hoe politie met **drones mogen vliegen, de inzet van bodycams, dashcams (**maar denk maar aan private 'slimme' Tesla's of (dure) Mercedes ECQ'sen die continu hun omgeving filmen, en meer).

Ze voorziet ook in de **uitbouw van het grote ANPR-netwerk.**

WAT MET PUBLIEKE RUIMTE?

Soms is de wet als een voorzienend: als een camera door een bepaalde hoek niet anders kan dan een deel van de openbare weg te filmen, dan dient er gebruik te worden gemaakt van *blurren:* het wazig maken is dan verplicht, door AI / algoritmes. Ook encryptie van de beelden is sowieso een vereiste (GDPR+Camerawet).

Controle hierop is echter… Onbestaand.



1,2 miljoen in Nederland

Ruim 1000 klachten in een jaar over slimme deurbel: 'Mensen voelen zich bespied'

23 februari 2024 12:20 • Aangepast 23 februari 2024 13:05

Net binnen

22:23 Matig Jong Oranje verliest in Nijmegen oefenduel van Noorwegen

22:20 Gaby Blaaser open over anorexia-verleden: 'SpangaS heeft me gered'

22:00 Secret Duets-partner Emma Heesters blijkt haar 'idool' uit tv-serie, maar hoe heet hij ook weer écht?

Darter Van Gerwen strandt voor de

De Autoriteit Persoonsgegevens (AP) maakt zich grote zorgen over het toenemende aantal privacyklachten over slimme deurbellen. In 2023 kreeg de AP 1050 meldingen binnen, een jaar eerder ging het nog om 800 meldingen.

De meldingen zijn van burgers die dachten dat een particuliere camera zoals een slimme deurbel in de buurt meer filmde dan is toegestaan. Dat bevestigt een woordvoerder van de toezichthouder na berichtgeving van de Volkskrant.

1,2 miljoen deurbellen

"Mensen voelen zich bespied als ze over straat lopen", zegt de woordvoerder. Ze gaat ervan uit dat steeds meer mensen zich ergeren aan het gevoel bespied te worden, omdat er steeds meer particuliere camera's als slimme deurbellen zijn.

Volgens marktonderzoeker Multiscope hingen er in Nederland in 2023 1,2 miljoen deurbellen met camera, tegenover 640.000 in 2021.

Lees ook:

'Medewerkers camerabedrijf Ring keken live bij

AP krijgt steeds meer vragen over videodeurbellen, hekelt houding van politie

De Autoriteit Persoonsgegevens kreeg vorig jaar meer dan duizend vragen en klachten van Nederlandse burgers over videodeurbellen. Het 'irriteert' de privacytoezichthouder dat de politie actief stimuleert zulke camera's op te hangen, zegt Aleid Wolfsen in de Volkskrant.

De Autoriteit Persoonsgegevens zegt tegen de Volkskrant dat zij vorig jaar 1050 telefoontjes van burgers kreeg die vragen stelden over deurbelcamera's in hun straat of wijk. Dat is een stijging van meer dan 200 vragen ten opzichte van een jaar ervoor. Volgens AP-voorzitter Aleid Wolfsen wordt 'het gros van de videodeurbellen' verkeerd opgehangen. Deurbellen mogen de openbare weg niet filmen, maar de AP zegt altijd dat het onvermijdelijk is dat een deel van de weg toch wordt gefilmd.

De AP hekelt de houding van de Nederlandse politie, die het juist vaak stimuleert om deurbelcamera's op te hangen. "Het lijkt soms alsof de politie het ophangen van die camera's juist aanmoedigt", zegt Wolfsen. "Dat irriteert ons." In 2019 ontdekte Tweakers al dat er meerdere Nederlandse gemeenten gratis deurbellen uitdeelden om criminaliteit tegen te gaan. Wolfsen denkt ook dat veel politieagenten denken dat videodeurbellen altijd mogen hangen. "Dat het in de rechtszaal als bewijs kan worden gebruikt, wekt de schijn dat die camera's daar rechtmatig hangen, terwijl dat niet zo is", zegt hij. De politie heeft in het verleden ook regelmatig actief gepleit voor het ophangen van deurbelcamera's.

In theorie kan de Autoriteit Persoonsgegevens handhaven als er een deurbel verkeerd is opgehangen en de privacy van de buren schendt. In België is dat al gebeurd: daar deelde de toezichthouder in 2020 een

Door **Tijs Hofma**
Nieuwscoördinat
Feedback

23-02-2024 • 15:12

REMINDER:

Onze straten hangen **vol met slimme deurbellen.** En toch blijft de vraag: kan je zomaar een *camera* installeren als particulier of bedrijf? Als de camera (of dus deurbel) niét gericht op de openbare weg, is er helemaal niets aan de hand: je mag altijd je private eigendom filmen, 24/24u. Daarbij moet je trouwens wél nog steeds bezoekers en zelfs werknemers informeren dat ze gefilmd worden (en hun rechten daarrond, zoals een dataverzoek of zelfs gegevenswissing).

Is de deurbel gericht **op de openbare weg**, dan is het een geheel ander verhaal. Springt de camera énkel aan bij het aanbellen, dan is er geen verschil met een klassieke deurbel met camera. Staat de slimme camera daarentegen de ganse dag te filmen (en dus de beelden te verwerken op een drager), **dan is het gebruik daarvan illegaal**. Dat er amper reactie op komt, is natuurlijk omdat de praktijk doorweegt op het juridische: boetes zijn er amper én de politie *vindt dit leuk*.

03. AI ACT & PRIVACY

Nieuwe wetgeving, nieuwe boetes

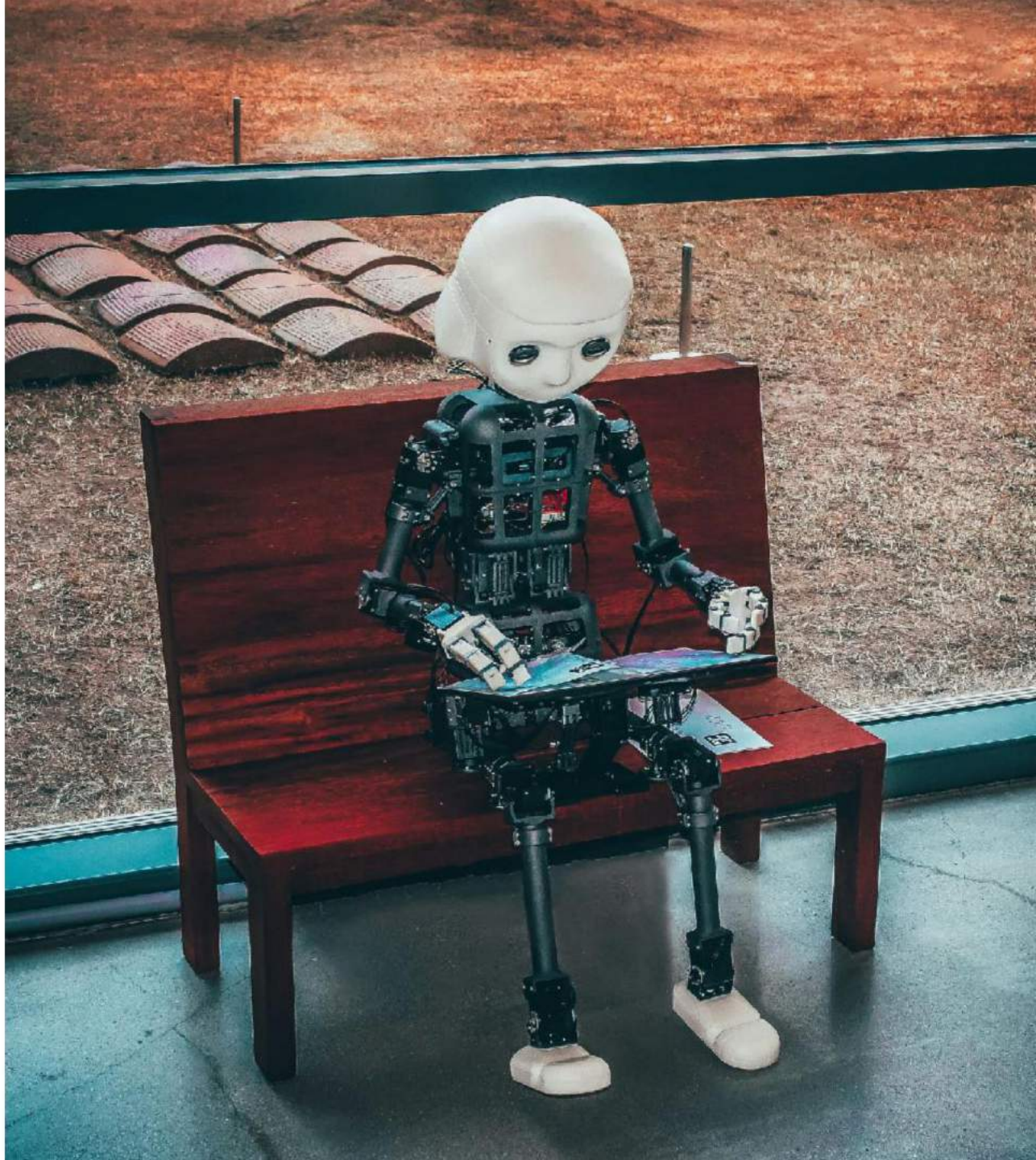
DOEL?

Het doel van de AI Act is dat mensen en bedrijven in de EU kunnen rekenen op **veilige, transparante, traceerbare, niet-discriminerende en milieuvriendelijke AI-systemen** die onder toezicht staan van mensen. Naar verwachting zal iedereen die met AI werkt vanaf 2026 moeten voldoen aan de eisen. De AI Act stelt h**oge boetes in het vooruitzicht voor overtreders. Tot 35 miljoen euro per overtreding of 7% van de wereldwijde omzet** van het concern waarbinnen de overtreding wordt gemaakt. Voor 'kleine', administratieve overtredingen is dit 7,5 miljoen of 1.5%.

TOEPASSING?

Alle inzet van AI (oftewel: autonoom werkende computers en algoritmes) **valt onder de AI Act.**

De verordening volgt een risicogebaseerde benadering en stelt **verplichtingen voor aanbieders en gebruikers afhankelijk van het risiconiveau** dat een AI-systeem met zich meebrengt. De AI Act is van toepassing op a**lle sectoren**, zoals de gezondheidszorg, overheid, financiën, het onderwijs en entertainment. De wet heeft een algemeen karakter en is niet beperkt tot een specifieke branche. Alleen bij inzet voor opsporings- en veiligheidsdiensten gelden aangepaste regels.

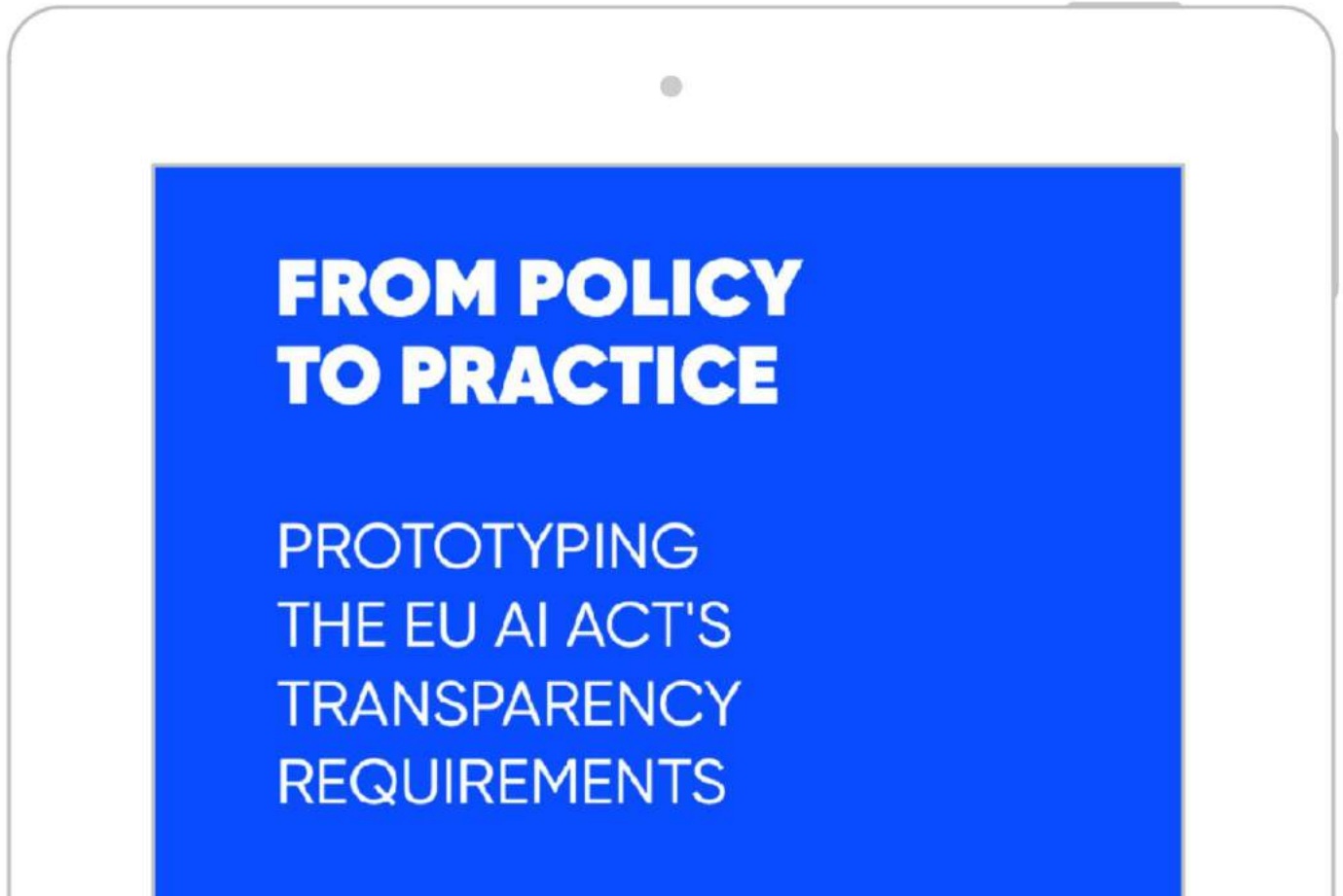


VOOR WIE?

De nieuwe regels gelden voor iedereen die AI ontwikkelt, op de markt brengt of inzet: producenten van AI-systemen, **integrators die AI in eigen softwarediensten opnemen**, importeurs die AI van buiten de EU halen en gebruikers die dergelijke diensten inzetten.

Iedereen die gebruik maakt van AI zal zelf moeten kunnen aantonen dat deze aan de regels voldoet, en zal dus **helderheid moeten opvragen bij de leverancier**.

KENNISCENTRUM DATA & MAATSCHAPPIJ



DATA BREACH

Datalekken en -hackings moeten nu verplicht worden aangemeld bij de GBA.

RIGHT TO BE FORGOTTEN

Je hebt nu het recht om te vragen aan bedrijven om je te ‘vergeten’.

DE AUTORITEIT

De privacycommissie werd de Gegevensbeschermingsautoriteit.

Overview lessons learned/best practices for disclaimers

General lessons learned/best practices

- **PROPORTIONALITY:** establish the desired level of transparency, taking into account the target audience and accessibility considerations. Develop and deploy a decision process that allows to identify which transparency tools are likely to achieve this objective in a timely, effective and proportionate manner. Consider that users seem to appreciate more than the strictly legally required information, but be cautious of providing too much information through too many channels.
- **ACCESSIBILITY:** Make sure the disclaimer is accessible to different users, taking into account users with disabilities. Follow established best practices and guidelines in this regard. This will probably imply that at least the disclaimer will have to be displayed in different forms (e.g. written, aural and (audio)visual)
- **TARGET AUDIENCE:** identify not only the intended but also the broader potential target audience to whom the disclaimer (and related information notices) may be presented. Avoid addressing the public in general and consider testing the design of the disclaimer (e.g. the avatar, icon or interface) with a focus group.
- **LANGUAGE:** Try to use clear, plain and concise language when drafting the disclaimer and the related information notices. Keep the target audience in mind when drafting the document.

Content-related lessons learned/best practices

- **USE A LAYERED APPROACH:** To optimize user engagement and avoid information overload, employing a layered approach in (information notices related to) the disclaimers might be effective. This method involves initially

RISICOKLASSEN

De systemen worden opgedeeld in **risicoklassen**: hoe **hoger** het risico, hoe **strenger** de vereisten.

Onaanvaardbaar risico: dit zijn AI-systemen die als een gevaar voor mensen worden beschouwd. Voorbeelden hiervan zijn het zogenaamde ‘social scoring’, en toepassing van bepaalde biometrische systemen voor identificatie op afstand zoals *gezichtsherkenning (!)*.

Hoog risico: deze AI-systemen brengen aanzienlijke risico's met zich mee en zullen aan strikte verplichtingen worden onderworpen voordat ze op de markt kunnen worden gebracht. Het overgrote deel van de verplichtingen uit de AI Act ziet op AI-systemen die hieronder vallen. Alle AI-systemen met een hoog risico krijgen een beoordeling voor zij in de handel worden gebracht en worden tijdens de volledige levensduur van het systeem gevolgd.

Laag risico: AI-systemen die niet in de bovenstaande categorieën vallen, mogen de Europese markt zonder al te veel problemen betreden. Er moet wel transparantie zijn, zodat het duidelijk is wanneer een beeld is gemanipuleerd (zogenaamde ‘deepfakes’) en niemand onterecht denkt dat hij of zij te maken heeft met een mens.

BOETES, BOETES.

De verordening stelt hoge boetes in het vooruitzicht voor overtreders. Deze kunnen oplopen tot **35 miljoen euro per overtreding of zeven procent** van de wereldwijde omzet van het betrokken concern.

Er moet trouwens ook een soort AI Autoriteit komen in België (nog ééntje ;-), naast de Gegevensbeschermingsautoriteit.

WELKE STAPPEN MOET JE ZETTEN?

Je kan nu al aan de slag gaan om je organisatie, en je technologie even kritisch te bekijken.

1

IN KAART BRENGEN

Breng alle AI-systemen in kaart die uw organisatie heeft ontwikkeld (of van plan is te ontwikkelen) of waarvan gebruik wordt gemaakt. Bepaal of een van deze systemen binnen de reikwijdte van de AI Act valt.

2

BEOORDELING

Beoordeel de AI-systemen die binnen de reikwijdte van de AI Act vallen om hun risicoclassificatie te bepalen en de toepasselijke nalevingseisen vast te stellen.

3

POSITIE

Begrijp de positie binnen relevante AI-waardeketens, de bijbehorende complianceverplichtingen en hoe aan deze verplichtingen zal worden voldaan.

4

PLAN

Stel een plan op om ervoor te zorgen dat de juiste verantwoordingsplicht en systemen aanwezig zijn wanneer de verordening van kracht wordt.

IMPACT OP ONZE PRIVACY?

De impact die AI op onze **privacy** zal hebben **valt niet te voorspellen** (of wel: het betert er niet op).

Hoewel de EU streng is voor bijvoorbeeld **gezichtsherkenning door politie (of, beter: door bedrijven)**, want sommige politiediensten kunnen op uitzonderingen rekenen, zullen **deepfakes, deepnudes** en allerlei **trucage** met (video)beelden zorgen voor bijzonder veel verwarring, én privacyinbreuken.

GEEN VERBOD OP DEEPFAKES.

Onbegrijpelijk, **maar er komt geen verbod vanuit de EU op deepfaketechnologie**.

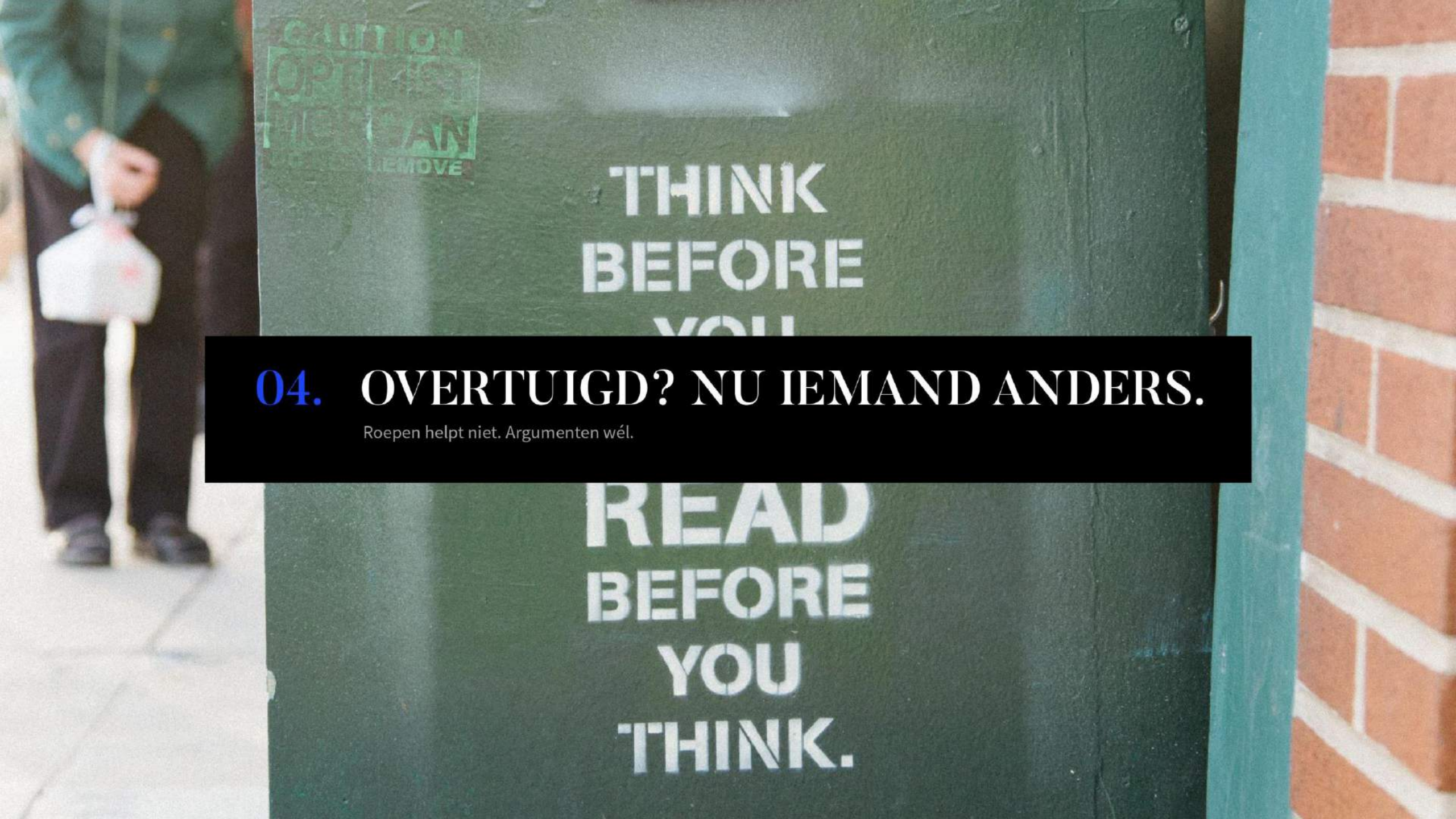
Technologie is meestal **neutraal:** hoewel ze kan misbruikt worden, levert technologie zeer veel voordelen op, zelfs bij intrusieve tech zoals camera's. Bij **deepfakes** ligt dat anders: er is **géén enkel voordeel vast te stellen.**

an Jean-Luc Dehaene © CD&V

Tex Van berlaer
Journalist Knack • 06-12-2023, 23:17 • Bijgewerkt op: 07-12-2023, 07:34 •

Met behulp van artificiële intelligentie heeft de CD&V oud-premier Jean-Luc Dehaene opnieuw tot leven gewekt. Het opzet getuigt van weinig goede smaak.

‘*The beast is back.*’ Met een parafrase van zijn beroemde boutad ‘*let the beast go*’ begint Jean-Luc Dehaene de kijker toe te spreken. ‘Respect werkt’, zegt hij op het einde. ‘Zeg dat de ervaren gids het gezegd heeft.’



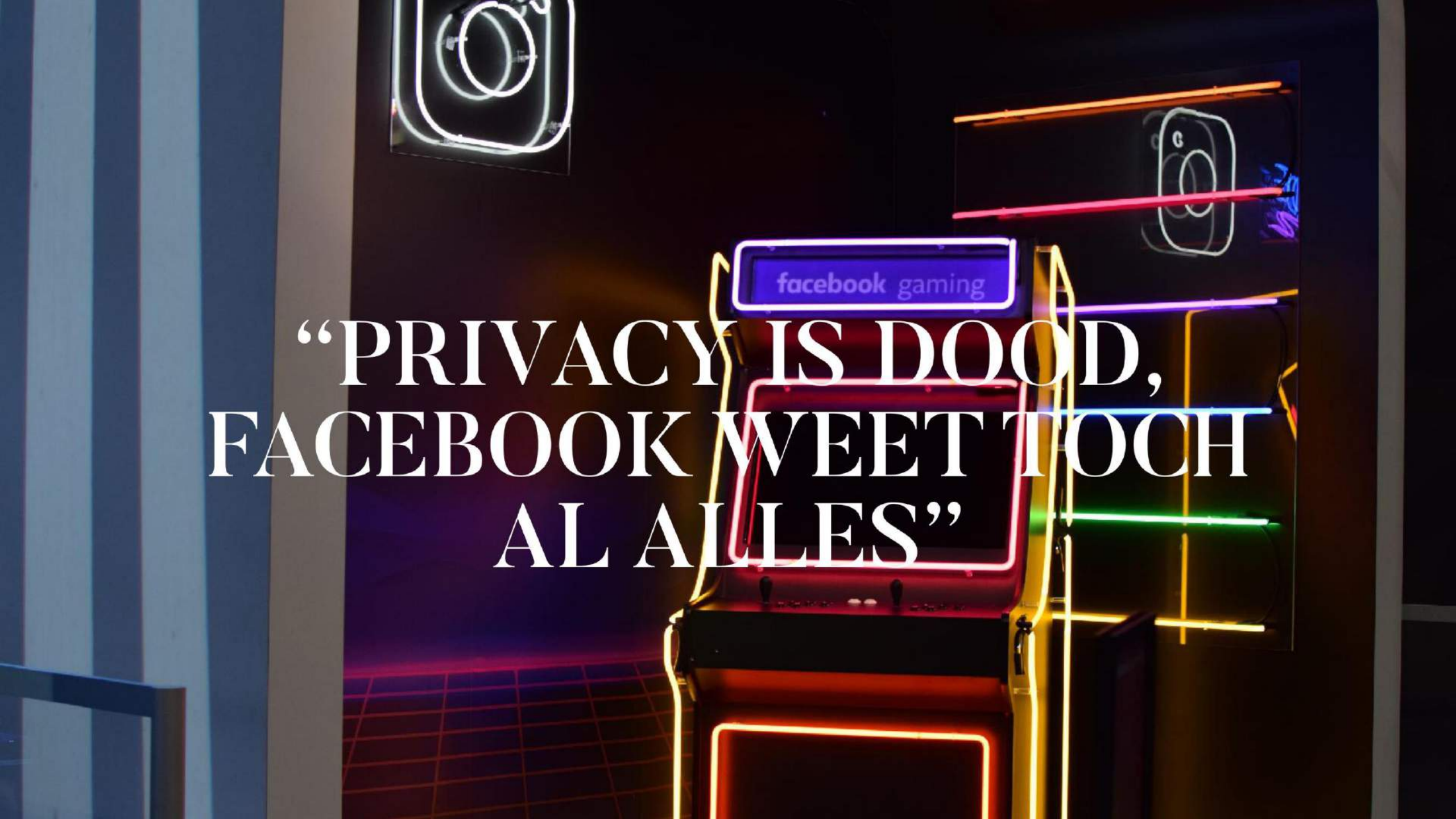
04. OVERTUIGD? NU IEMAND ANDERS.

Roepen helpt niet. Argumenten wél.

GDPRGRRR

“IK HEB NIETS TE VERBERGEN”


“ALS JE NIETS
VERKEERD DOET, HEB JE
NIETS TE VREZEN”



“PRIVACY IS DOOD, FACEBOOK WEET TOCH AL ALLES”


“MIJN GEZONDHEID/
VEILIGHEID GAAT VOOR
OP PRIVACY”

BAD ARGUMENTS ARE HERE TO STAY.

JE KAN NIET IEDEREEN OVERTUIGEN.

Zolang het debat sluimert, zal een gebrekkig argument vallen. Je zal nooit iedereen kunnen overtuigen, maar dat is ook niet nodig. Wat wél nodig is, is om het **privacydebat naar een hoger niveau te tillen**, en weg te stappen van de dooddoeners die we net zagen. Een kritische massa, de droom van elke privacy-activist.

05. ‘MAAR WAAROM ZAAG JE ZOVEEL’

Voorbeelden genoeg

Krant Avond Weekblad Magazine Letteren Webshop Klas

De Standaard Nieuws Opinie Inspiratie Podcasts

Opinies Columns

DE MENING

Verdient uw privacy meer bescherming dan een kind?

Marc Dutroux. — © belga/afp

HLN NIEUWS SPORT SHOWBIZZ NINA REGIO VIDEO PUZZEL PODC

Opinie Geld Eten Tech Mobiliteit Gezondheid Wonen Reizen Wetenschap & Plan

Komen er binnenkort 10.000 ANPR-camera's? Cryptograaf Bart Preneel blikt vooruit. © ThinkStock / BV

"Privacy zal in de toekomst enkel voor de rijken zijn": twee Vlaamse experts waarschuwen voor onze afkalvende privacy

HLN NIEUWS SPORT SHOWBIZZ NINA REGIO VIDEO PUZZEL PODC

Vingerafdrukken op identiteitskaarten schenden privacy niet

De verplichting om twee vingerafdrukken op te nemen op elektronische identiteitskaarten gaat niet in tegen het recht op privacy. Dat concludeert het Europees Hof van Justitie in een arrest. De Europese verordening die de verplichting regelt moet niettemin op de schop, omdat ze gebaseerd is op "een onjuiste rechtsgrondslag".

Redactie 21-03-24, 12:41

12 REACTIES

De zaak werd aanhangig gemaakt door een Duitser, die naar de rechter stapte nadat de stad Wiesbaden hem geen nieuwe identiteitskaart zonder vingerafdrukken wilde geven. In de EU zijn elektronische identiteitskaarten met digitale vingerafdrukken sinds enkele jaren immers verplicht, maar volgens de Duitser in kwestie gaat dat in tegen de privacybescherming. Een Duitse rechter speelde de vraag door aan het Europees Hof van Justitie.

Dat oordeelt nu dat de verplichte vingerafdrukken op elektronische

English Newsletters Podcasts Events Jobs Login/Register Search

EURACTIV

Home / News / Technology / Artificial Intelligence / Italian data protection authority bans ChatGPT citing privacy violations

Italian data protection authority bans ChatGPT citing privacy violations

By Luca Bertuzzi | Euractiv.com Est. 4min 31 mrt 2023 (updated: 13 apr 2023)

HLN NIEUWS SPORT SHOWBIZZ NINA REGIO VIDEO PUZZEL PODCAST SERVICE

minister van Binnenlandse Zaken Annelies Verlinden (CD&V). © ID/ Dries Luyten / BELGA

Federale politie kan ANPR-netwerk uitbouwen tot 10.000 camera's

De federale politie kan haar netwerk van camera's met nummerplaatherkenning op termijn uitbouwen tot 10.000 met elkaar verbonden ANPR-camera's. Dat heeft de federale regering beslist bij de begrotingsopmaak van 2024.

Redactie 10-10-23, 12:54

45 REACTIES

van ernstige nieuwe elementen": Roger...

Waalse buschauffeur vermoord met zestien messteken, collega ont

"Door hoogste pensioen te verlagen, kunnen mensen met een zwaar

Familie van 17-jarige fie reageert na vluchtmisd "Het beeld van mijn zoo

“

Hey you...

Thank you for having me.
Good luck.

alia
connecting security interests

Bedankt voor je aandacht

Merci pour votre attention

Nelectra
Federatie voor de elektrosector

ELOYA
union des électriciens
unie van elektriciens

Techlink
Linking technicians

FEE

ANPI

NEW SECURITY MAGAZINE

connecting security interests

SAVE THE DATE

ALIA Security Day 2025