DOC 56 **0601/001**

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

17 december 2024

# WETSVOORSTEL

**tot invoeging van een nieuw artikel in het Wetboek van Strafvordering ter uitvoering van artikel 5, lid 5, van Verordening (EU) 2024/1689 betreffende artificiële intelligentie**

(ingediend door de heer Paul Van Tigchelt)

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

17 décembre 2024

# PROPOSITION DE LOI

**insérant un nouvel article dans le Code d'instruction criminelle afin de mettre en oeuvre l'article 5, paragraphe 5, du Règlement (UE) 2024/1689 sur l'intelligence artificielle**

(déposée par M. Paul Van Tigchelt)

**SAMENVATTING**

*Dit wetvoorstel is bedoeld om artikel 5, lid 5, van de Verordening (EU) 2024/1689 betreffende artificiële intelligentie (AI) uit te voeren. Het beoogt de toepassing van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving mogelijk te maken. Dit moet gebeuren onder de strikte voorwaarden die zijn vastgelegd in de bovenvermelde Verordening.*

*Het doel van die Verordening is tweeledig. Enerzijds de toepassing van betrouwbare AI in Europa te bevorderen en de bescherming van de gezondheid, de veiligheid en de grondrechten van individuen te waarborgen, en anderzijds innovatie in AI te ondersteunen. Deze Verordening heeft brede impact op publieke en private actoren, zowel binnen als buiten de EU, die AI-systemen op de Europese markt brengen of gebruiken.*

**RÉSUMÉ**

*La présente proposition de loi vise à mettre en œuvre l'article 5, paragraphe 5, du Règlement (UE) 2024/1689 sur l'intelligence artificielle (IA). La proposition vise à autoriser l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives. Cela doit se faire dans les conditions strictes prévues par le Règlement susmentionné.*

*Le Règlement poursuit un objectif double. D'une part, promouvoir l'adoption d'une intelligence artificielle axée sur l'humain et digne de confiance, tout en garantissant la protection de la santé, la sécurité et les droits fondamentaux des citoyens contre les risques potentiels de l'IA et, d'autre part, soutenir l'innovation dans le domaine de l'IA.Ce règlement a un large impact sur les acteurs publiques et privés, tant à l'intérieur qu'à l'extérieur de l'UE, qui mettent sur le marché européen ou utilisent des systèmes d'IA.*

| | | |
|---|---|---|
| *N-VA* | : | *Nieuw-Vlaamse Alliantie* |
| *VB* | : | *Vlaams Belang* |
| *MR* | : | *Mouvement Réformateur* |
| *PS* | : | *Parti Socialiste* |
| *PVDA-PTB* | : | *Partij van de Arbeid van België – Parti du Travail de Belgique* |
| *Les Engagés* | : | *Les Engagés* |
| *Vooruit* | : | *Vooruit* |
| *cd&v* | : | *Christen-Democratisch en Vlaams* |
| *Ecolo-Groen* | : | *Ecologistes Confédérés pour l'organisation de luttes originales – Groen* |
| *Open Vld* | : | *Open Vlaamse liberalen en democraten* |
| *DéFI* | : | *Démocrate Fédéraliste Indépendant* |

| *Abréviations dans la numérotation des publications:* | | *Afkorting bij de nummering van de publicaties:* | |
|---|---|---|---|
| *DOC 56 0000/000* | *Document de la 56e législature, suivi du numéro de base et numéro de suivi* | *DOC 56 0000/000* | *Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer* |
| *QRVA* | *Questions et Réponses écrites* | *QRVA* | *Schriftelijke Vragen en Antwoorden* |
| *CRIV* | *Version provisoire du Compte Rendu Intégral* | *CRIV* | *Voorlopige versie van het Integraal Verslag* |
| *CRABV* | *Compte Rendu Analytique* | *CRABV* | *Beknopt Verslag* |
| *CRIV* | *Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)* | *CRIV* | *Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)* |
| *PLEN* | *Séance plénière* | *PLEN* | *Plenum* |
| *COM* | *Réunion de commission* | *COM* | *Commissievergadering* |
| *MOT* | *Motions déposées en conclusion d'interpellations (papier beige)* | *MOT* | *Moties tot besluit van interpellaties (beigekleurig papier)* |

## TOELICHTING

DAMES EN HEREN,

Dit wetvoorstel beoogt artikel 5, lid 5, van de Verordening (EU) 2024/1689[1] artificiële intelligentie (hierna "de Verordening"), gepubliceerd in het *Publicatieblad van de Europese Unie* op 12 juli 2024, ten uitvoer te leggen. Het beoogt het gebruik toe te laten van systemen voor biometrische identificatie op afstand in real time bedoeld in artikel 3, 42), van de Verordening (EU) 2024/1689 in openbare ruimten met het oog op de rechtshandhaving en dit overeenkomstig de grenzen en voorwaarden van artikel 5, lid 1, eerste alinea, punt h), en de leden 2 tot 4 en 6 van de Verordening.

Het doel van de Verordening is tweeledig: enerzijds de toepassing van mensgerichte en betrouwbare artificiële intelligentie (hierna "AI") bevorderen in Europa, door ervoor te zorgen dat de gezondheid, de veiligheid en de grondrechten van individuen worden beschermd tegen de mogelijke risico's van AI, en anderzijds innovatie op het gebied van AI ondersteunen.

Het betreft een horizontale verordening, die een grote impact heeft op zowel publieke als particuliere actoren, zowel in de Europese Unie als daarbuiten, die een AI-systeem voor een specifiek doel of gebruik in de handel brengen, in gebruik stellen of gebruiken in de Europese Unie, of wanneer de output van een AI-systeem in de Unie wordt gebruikt.

Met deze Verordening wil de Europese Unie een voortrekkersrol spelen bij de ontwikkeling van veilige, betrouwbare en ethische AI.

De Verordening introduceert een definitie van een "AI-systeem", dat gebaseerd is op de internationale OESO-definitie.

De Verordening volgt een risicogebaseerde aanpak, dit wil zeggen dat hoe groter de risico's van een AI-systeem zijn, hoe strenger de toepasselijke regels ook zullen zijn. Binnen dit kader introduceert de Verordening vier risiconiveaus voor AI-systemen en identificeert ze ook zogenaamde "systeemrisico"s' specifiek voor AI-modellen voor algemene doeleinden:

[1] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (Voor de EER relevante tekst).

## DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition de loi vise à mettre en œuvre l'article 5, paragraphe 5, du Règlement (UE) 2024/1689[1] sur l'intelligence artificielle (ci-après "le Règlement"), qui a été publié le 12 juillet 2024 dans le *Journal Officiel de l'Union Européenne*. Il vise à autoriser l'utilisation de systèmes d'identification biométrique à distance en temps réel visés par l'article 3, 42), du Règlement (UE) 2024/1689 dans des espaces accessibles au public à des fins répressives selon des limites et des conditions conformes à celles énumérées à l'article 5, paragraphe 1er, premier alinéa, point h), et aux paragraphes 2 à 4 et 6 du Règlement.

Le Règlement poursuit un objectif double: d'une part, promouvoir l'adoption d'une intelligence artificielle (ci-après "IA") axée sur l'humain et digne de confiance, tout en garantissant la protection de la santé, la sécurité et les droits fondamentaux des citoyens contre les risques potentiels de l'IA et, d'autre part, soutenir l'innovation dans le domaine de l'IA.

C'est un règlement horizontal, qui a un grand impact sur les acteurs publics et privés, tant au sein de l'Union européenne qu'en dehors de celle-ci, qui mettent sur le marché, mettent en service ou utilisent un système d'IA à une fin ou une utilisation spécifique dans l'Union européenne, ou lorsque les sorties d'un système d'IA sont utilisées dans l'Union, ou lorsque les résultats d'un système d'IA sont utilisés dans l'Union.

Grâce à ce Règlement, l'Union européenne entend assumer un rôle de premier plan dans le développement d'une IA sûre, digne de confiance et éthique.

Le Règlement introduit une définition de "système d'IA" basée sur la définition internationale de l'OCDE.

Ce Règlement suit une approche fondée sur les risques: plus les risques d'un système d'IA sont élevés, plus les règles applicables sont strictes. Le Règlement introduit quatre niveaux de risque pour les systèmes d'IA et identifie également lesdits "risques systémiques" spécifiquement pour les modèles d'IA à usage général:

[1] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (Texte présentant de l'intérêt pour l'EEE).

1. onaanvaardbaar risico: sommige AI-systemen schenden de grondrechten en de waarden van de Europese Unie waardoor ze verboden zullen zijn, bijvoorbeeld "sociale scoring" van individuen en gedragsmanipulatie van kwetsbare groepen die leidt tot aanzienlijke schade, zoals een AI-gegenereerde stem in speelgoed die gevaarlijk gedrag uitlokt bij kinderen;

2. hoog risico: AI-systemen met een hoog risico zijn toegelaten, zolang ze voldoen aan bepaalde strenge dwingende eisen, met inbegrip van een *ex ante* conformiteitsbeoordeling. Een AI-systeem met een hoog risico is een AI-systeem dat aanzienlijke schadelijke gevolgen kan hebben voor de gezondheid, de veiligheid en de grondrechten van personen in de Europese Unie. Om deze schadelijke gevolgen te voorkomen gelden de meeste verplichtingen uit hoofde van de Verordening voor de aanbieders (*providers*) en gebruiksverantwoordelijken (*deployers*) van deze hoog risico AI-systemen. In het bijzonder Bijlage III van de Verordening bevat een lijst van acht gebieden waarin AI-toepassingen worden geacht hoge risico's met zich mee te brengen. Voorbeelden van dergelijke AI-toepassingen zijn het gebruik van AI bij de aanwerving van werknemers, bijvoorbeeld voor het screenen en beoordelen van cv's, en AI-tools voor de evaluatie van de kredietwaardigheid van natuurlijke personen die bijvoorbeeld een lening willen aangaan;

3. beperkt risico of transparantierisico: voor deze categorie AI-systemen gelden er enkele informatie- en transparantieverplichtingen met als doel het vertrouwen te bevorderen. Gebruikers van chatbots moeten zich er bijvoorbeeld van bewust zijn dat zij interageren met een machine in plaats van met een mens, zodat ze een weloverwogen beslissing kunnen nemen om door te gaan of een stap terug te doen;

4. minimaal risico of geen risico: de overgrote meerderheid van de AI-systemen die momenteel in de Europese Unie worden gebruikt, vallen in deze categorie, bijvoorbeeld AI-gestuurde videogames of spamfilters, waarvoor geen specifieke verplichtingen gelden krachtens de Verordening;

5. AI-modellen voor algemene doeleinden (GPAI) met systeemrisico's ("tweetrapsbenadering"): sommige GPAI-modellen kunnen systeemrisico's met zich meebrengen als ze zeer krachtig zijn en op grote schaal worden gebruikt. Voor de aanbieders van dit soort modellen gelden bepaalde specifieke transparantieverplichtingen, zoals het bijhouden van technische documentatie van het model en het opstellen van een beleid voor de naleving van het Unierecht inzake auteursrechten, en daarbovenop zijn er bijkomende verplichtingen, zoals het uitvoeren

1. risque inacceptable: certains systèmes d'IA violent les droits fondamentaux et les valeurs de l'Union européenne. Ces systèmes d'IA seront interdits. Il peut par exemple s'agir de "*social scoring*" des individus et de manipulation du comportement de groupes vulnérables entraînant des dommages importants, comme une voix générée par l'IA dans les jouets qui déclenche un comportement dangereux chez les enfants;

2. haut risque: les systèmes d'IA à haut risque sont autorisés dans l'Union pour autant qu'ils satisfassent à certaines exigences contraignantes strictes, y compris à une évaluation *ex ante* de la conformité. Un système d'IA à haut risque est un système d'IA qui peut avoir une incidence préjudiciable significative sur la santé, la sécurité et les droits fondamentaux des citoyens dans l'Union européenne. Pour prévenir ces conséquences néfastes, la plupart des obligations prévues au titre du Règlement s'appliquent aux fournisseurs (*providers*) et aux déployeurs (*deployers*) de systèmes d'IA à haut risque. En particulier, l'annexe III du Règlement contient une liste de huit domaines dans lesquels les applications d'IA sont réputées à haut risque. Des exemples de telles applications d'IA sont l'utilisation de l'IA lors du recrutement de travailleurs, par exemple pour la sélection et l'évaluation des CV, et les outils d'IA pour évaluer la solvabilité des personnes physiques souhaitant, par exemple, contracter un prêt;

3. risque limité ou de transparence: cette catégorie de systèmes d'IA est soumise à certaines obligations en matière d'information et de transparence dans le but de favoriser la confiance. Les utilisateurs de chatbots doivent être conscients, par exemple, qu'ils interagissent avec une machine et non avec un humain, de sorte qu'ils puissent décider en connaissance de cause de poursuivre ou de revenir;

4. risque minimal ou nul: la grande majorité des systèmes d'IA qui sont actuellement utilisés dans l'Union européenne relèvent de cette catégorie, par exemple les jeux vidéo pilotés par l'IA ou les filtres anti-spam, qui ne sont soumis à aucune obligation spécifique au titre du Règlement;

5. modèles d'IA à usage général (GPAI) avec risques systémiques ("approche en deux étapes"): certains modèles GPAI peuvent présenter des risques systémiques s'ils sont très puissants et utilisés à grande échelle. Des obligations de transparence s'appliquent aux fournisseurs de ce type de modèles, comme la tenue de la documentation technique du modèle et l'élaboration d'une politique de respect du droit de l'Union en matière de droits d'auteur, ainsi que des obligations supplémentaires telles que la réalisation d'une évaluation

van een evaluatie van het model en het beoordelen en beperken van mogelijke systeemrisico's op Unieniveau.

De Verordening zal niet van toepassing zijn op AI in het kader van *research & development*, AI voor militaire doeleinden, defensiedoeleinden en nationale veiligheidsdoeleinden, AI gebruikt in het kader van een persoonlijke, niet-professionele activiteit en kosteloze en open source GPAI-modellen, behalve wanneer systeemrisico's zich voordoen.

De Verordening is in werking getreden op 1 augustus 2024.

De inwerkingtredingsbepaling (artikel 113 van de Verordening) bepaalt:

"Zij is van toepassing met ingang van 2 augustus 2026.

Evenwel zijn:

a) de hoofdstukken I en II van toepassing met ingang van 2 februari 2025;

b) hoofdstuk III, afdeling 4, hoofdstuk V, hoofdstuk VII en hoofdstuk XII en artikel 78 van toepassing met ingang van 2 augustus 2025, met uitzondering van artikel 101;

c) artikel 6, lid 1, en de overeenkomstige verplichtingen van deze verordening van toepassing met ingang van 2 augustus 2027.".

Uit het voorgaande volgt dat met ingang van 2 februari 2025 de algemene bepalingen en de bepalingen rond verboden AI-praktijken, zoals vervat in artikel 5 van de Verordening van toepassing zullen zijn.

Artikel 5 van de Verordening verbiedt het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving tenzij en voor zover een dergelijk gebruik strikt noodzakelijk is voor een van de in artikel 5, lid 1, eerste alinea, h), vermelde doelstellingen.

Artikel 5, vijfde lid, van de Verordening bepaalt dat: "Een lidstaat kan besluiten om te voorzien in de mogelijkheid om volledig of gedeeltelijk toestemming te verlenen voor het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving binnen de grenzen en onder de voorwaarden van lid 1, eerste alinea, punt h), en de leden 2 en 3. De betrokken lidstaten leggen in hun nationale recht de noodzakelijke gedetailleerde regels vast voor het verzoek om en de afgifte en het gebruik van, evenals het toezicht en verslaglegging in verband met, de in lid 3 bedoelde vergunningen. In deze regels

du modèle, mais aussi l'évaluation et l'atténuation de risques systémiques éventuels au niveau de l'Union.

Le Règlement ne s'appliquera pas à l'IA dans le cadre de la recherche et du développement, à l'IA à des fins militaires, de défense et de sécurité nationale, à l'IA utilisée dans le cadre d'une activité personnelle et non professionnelle et aux modèles GPAI gratuits et open source, sauf lorsque des risques systémiques apparaissent.

Le Règlement est entré en vigueur le 1er août 2024.

La disposition d'entrée en vigueur (article 113 du Règlement) prévoit:

"Il est applicable à partir du 2 août 2026.

Toutefois:

a) les chapitres I et II sont applicables à partir du 2 février 2025;

b) le chapitre III, section 4, le chapitre V, le chapitre VII, le chapitre XII et l'article 78 s'appliquent à partir du 2 août 2025, à l'exception de l'article 101;

c) l'article 6, paragraphe 1, et les obligations correspondantes du présent règlement s'appliquent à partir du 2 août 2027.".

Il résulte de ce qui précède qu'à compter du 2 février 2025, les dispositions générales et les dispositions relatives aux pratiques interdites en matière d'IA, telles que contenues à l'article 5 du Règlement, s'appliqueront.

L'article 5 du Règlement interdit l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs énumérés dans l'article 5, premier alinéa, point h).

L'article 5, paragraphe 5, du Règlement dispose ce qui suit: "Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, dans les limites et les conditions énumérées au paragraphe 1, premier alinéa, point h), et aux paragraphes 2 et 3. Les États membres concernés établissent dans leur droit national les règles détaillées nécessaires à la demande, à la délivrance et à l'exercice des autorisations visées au paragraphe 3, ainsi qu'à la surveillance et à l'établissement de rapports

wordt ook gespecificeerd voor welke doelstellingen van lid 1, eerste alinea, punt h), en voor welke strafbare feiten als bedoeld in punt h), iii), daarvan de bevoegde autoriteiten deze systemen mogen gebruiken met het oog op de rechtshandhaving. De lidstaten stellen de Commissie uiterlijk dertig dagen na de vaststelling van die regels in kennis. De lidstaten kunnen in overeenstemming met het Unierecht restrictievere wetgeving inzake het gebruik van systemen voor biometrische identificatie op afstand invoeren.".

Dit wetvoorstel beoogt deze bepaling ten uitvoer te leggen.

Vooraleer gedetailleerd in te gaan op de aanvullende informatie in de consideransen van de Verordening, is het goed om erop te wijzen dat dit Europese instrument is opgesteld in een andere sector van de Raad van de Europese Unie dan deze van justitie en binnenlandse zaken Aangezien dit instrument door de Europese Commissie werd opgevat als een horizontaal instrument, werd de voorbereiding van het standpunt van de Raad toevertrouwd aan de Groep telecommunicatie en informatiemaatschappij (Telecom) in het kader van de Vervoer/Telecommunicatie/Energie raadsformatie, terwijl de voorbereiding van het standpunt van het Europees Parlement werd toevertrouwd aan de Commissie interne markt en consumentenbescherming (IMCO) en de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE). De Justitie en Binnenlandse Zaken (JBZ) raadsformatie werd in een later stadium bij de onderhandelingen betrokken en het vooruitzicht van een specifieke sectorale tekst voor de JBZ-sector werd in dat stadium uitgesloten. Het is in deze bijzondere context dat rekening is gehouden met de bezorgdheden van de terreinactoren die betrokken zijn bij ordehandhaving en het strafrecht.

Het gebruik van biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving was een van de meest controversiële kwesties tijdens de trialogen; er was grote druk van voorstanders van de privacy binnen het Europees Parlement. Het resultaat is een vrij restrictieve tekst voor de publieke actoren.

Dit ontwerp sluit zo nauw mogelijk aan bij de tekst zelf van de Verordening.

Het in de verordening vastgestelde evenwicht tussen de bescherming van de grondrechten en de operationele vereisten van een doeltreffend strafrechtelijk onderzoek wordt aldus zo goed mogelijk in acht genomen.

Artikel 3, 42), van de Verordening definieert een systeem voor biometrische identificatie op afstand in real time

y afférents. Ces règles précisent également pour quels objectifs énumérés au paragraphe 1, premier alinéa, point h), et notamment pour quelles infractions pénales visées au point h), iii), les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives. Les États membres notifient ces règles à la Commission au plus tard 30 jours après leur adoption. Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance.".

La présente proposition de loi a pour objectif de mettre en œuvre cette disposition.

Avant de détailler les indications supplémentaires que fournissent les considérants du Règlement, il est utile de préciser que cet instrument européen a été élaboré dans une autre filière du Conseil de l'Union européenne que celle de la justice et des affaires intérieures. En effet, comme cet instrument a été conçu par la Commission européenne comme un instrument horizontal, la préparation de la position du Conseil a été confiée au groupe de travail Télécommunication et Société de l'information (Telecom) au sein de la formation du Conseil Transports / Télécommunications / Énergie alors que la préparation de la position du Parlement européen a été confiée à la Commission du marché intérieur et de la protection des consommateurs (IMCO) et à la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE). La filière Justice et Affaires intérieures (JAI) a été associée dans un stade ultérieur de la négociation et la perspective d'un texte sectoriel spécifique pour la filière JAI a été écartée à ce stade-là. C'est dans ce contexte particulier que les préoccupations des acteurs de terrain en matière de maintien de l'ordre et de justice pénale ont été aménagées.

L'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives a fait partie des questions les plus controversées durant les trilogues; il y avait une forte pression venant des défenseurs de la vie privée au sein du Parlement européen. Il en résulte un texte assez restrictif pour les acteurs publics.

Ce projet s'appuie le plus possible sur le texte-même du Règlement.

L'équilibre qu'établit le Règlement entre la protection des droits fondamentaux et les nécessités opérationnelles d'une enquête pénale efficace y est ainsi respecté au plus près.

L'article 3, 42), du Règlement définit un système d'identification biométrique à distance en temps réel

als volgt: “een systeem voor biometrische identificatie op afstand, waarbij het vastleggen van biometrische gegevens, de vergelijking en de identificatie zonder significante vertraging plaatsvinden, zowel wanneer de identificatie niet enkel onmiddellijk plaatsvindt, maar ook wanneer de identificatie met beperkte korte vertragingen plaatsvindt, om omzeiling te voorkomen”.

Overweging 15 bepaalt dat het in deze verordening bedoelde begrip “biometrische identificatie” moet worden gedefinieerd als de automatische herkenning van fysieke, fysiologische en gedragsgerelateerde menselijke kenmerken zoals het gezicht, de oogbewegingen, de lichaamsvorm, de stem, de prosodie, de gang, de houding, de hartslag, de bloeddruk, de geur, de toetsaanslagen, met als doel de identiteit van een natuurlijke persoon vast te stellen door biometrische gegevens van die natuurlijke persoon te vergelijken met opgeslagen biometrische gegevens van natuurlijke personen in een referentiedatabank, ongeacht of die natuurlijke persoon daarmee heeft ingestemd. Daarvan uitgesloten zijn AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie, met inbegrip van authenticatie, die er uitsluitend op gericht zijn te bevestigen dat een specifieke natuurlijke persoon daadwerkelijk de persoon is die hij of zij beweert te zijn, en de identiteit van een natuurlijke persoon te bevestigen met als enige doel toegang te verschaffen tot een dienst, een apparaat te ontgrendelen of beveiligde toegang te verschaffen tot een locatie.

Overweging 32 bepaalt dat het gebruik van AI-systemen voor biometrische identificatie op afstand in real time van natuurlijke personen in openbare ruimten voor rechtshandhavingsdoeleinden als bijzonder ingrijpend wordt beschouwd voor de rechten en vrijheden van de betrokkenen, in die mate dat het de persoonlijke levenssfeer van een groot deel van de bevolking kan aantasten, een gevoel van voortdurende bewaking kan oproepen en indirect de uitoefening van de vrijheid van vergadering en andere grondrechten kan ontmoedigen. Technische onnauwkeurigheden van AI-systemen voor biometrische identificatie op afstand van natuurlijke personen kunnen tot vertekende resultaten en discriminerende effecten leiden. Dergelijke mogelijke vertekende resultaten en discriminerende effecten zijn met name relevant met betrekking tot de leeftijd, de etniciteit, het ras, het geslacht of de handicap. Bovendien houden het directe karakter van de gevolgen en de beperkte mogelijkheden voor verdere controles of correcties met betrekking tot het gebruik van dergelijke realtimesystemen, verhoogde risico’s in voor de rechten en vrijheden van de betrokken personen in de context van rechtshandhavingsactiviteiten of wanneer die personen van de rechtshandhavingsactiviteiten gevolgen ondervinden.

comme suit: “un système d’identification biométrique à distance dans lequel l’acquisition des données biométriques, la comparaison et l’identification se déroulent sans décalage temporel important et qui comprend non seulement l’identification instantanée, mais aussi avec un léger décalage afin d’éviter tout contournement des règles”.

Le considérant 15 prévoit que la notion d’“identification biométrique” visée dans le présent règlement devrait être définie comme la reconnaissance automatisée de caractéristiques physiques, physiologiques et comportementales d’une personne, telles que le visage, les mouvements oculaires, la forme du corps, la voix, la prosodie, la démarche, la posture, le rythme cardiaque, la pression sanguine, l’odeur et la frappe au clavier, aux fins d’établir l’identité d’une personne par comparaison des données biométriques de cette personne avec les données biométriques de personnes stockées dans une base de données de référence, que la personne ait donné son approbation ou non. En sont exclus les systèmes d’IA destinés à être utilisés à des fins de vérification biométrique, ce qui inclut l’authentification, dont la seule finalité est de confirmer qu’une personne physique donnée est bien celle qu’elle prétend être et de confirmer l’identité d’une personne physique dans le seul but d’avoir accès à un service, de déverrouiller un dispositif ou de disposer d’un accès sécurisé à des locaux.

Le considérant 32 prévoit que l’utilisation de systèmes d’IA pour l’identification biométrique à distance “en temps réel” de personnes physiques dans des espaces accessibles au public à des fins répressives est particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d’une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l’exercice de la liberté de réunion et d’autres droits fondamentaux. Les inexactitudes techniques des systèmes d’IA destinés à l’identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Ce risque de résultats biaisés et d’effets discriminatoires est particulièrement significatif en ce qui concerne l’âge, l’appartenance ethnique, la race, le sexe ou le handicap. En outre, du fait de l’immédiateté des effets et des possibilités limitées d’effectuer des vérifications ou des corrections supplémentaires, l’utilisation de systèmes fonctionnant en temps réel engendre des risques accrus pour les droits et les libertés des personnes concernées dans le cadre d’activités répressives ou affectées par celles-ci.

Overweging 33 bepaalt dat het gebruik van dergelijke systemen voor rechtshandhavingsdoeleinden derhalve moet worden verboden, behalve in limitatief opgesomde en nauwkeurig omschreven situaties, waarin het gebruik strikt noodzakelijk is om een zwaarwegend algemeen belang te dienen, dat zwaarder weegt dan de risico's. Die situaties hebben betrekking op de zoektocht naar bepaalde slachtoffers van misdrijven, waaronder vermiste personen; bepaalde bedreigingen ten aanzien van het leven of de fysieke veiligheid van natuurlijke personen of van een terroristische aanslag, en de lokalisatie of identificatie van daders of verdachten van de in een bijlage bij deze verordening genoemde strafbare feiten, indien die strafbare feiten in de betrokken lidstaat strafbaar zijn gesteld met een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel met een maximumduur van ten minste vier jaar en zoals zij zijn gedefinieerd in het recht van die lidstaat. Een dergelijke drempel voor de vrijheidsstraf of de tot vrijheidsbeneming strekkende maatregel overeenkomstig het nationale recht helpt erop toe te zien dat het strafbare feit ernstig genoeg is om het gebruik van systemen voor biometrische identificatie op afstand in real time te rechtvaardigen. De in een bijlage bij deze verordening genoemde strafbare feiten zijn gebaseerd op de 32 in het Kaderbesluit 2002/584/JBZ van de Raad genoemde strafbare feiten, ermee rekening houdend dat sommige van die strafbare feiten in de praktijk waarschijnlijk relevanter zijn dan andere, aangezien het gebruik van biometrische identificatie op afstand in real time naar verwachting in zeer uiteenlopende mate noodzakelijk en evenredig zou kunnen zijn voor de praktische uitvoering van de lokalisatie of identificatie van een dader of verdachte van de verschillende opgesomde strafbare feiten, gelet op de te verwachten verschillen in ernst, waarschijnlijkheid en omvang van de schade of de mogelijke negatieve gevolgen. Een imminente dreiging voor het leven of de fysieke veiligheid van natuurlijke personen kan ook het gevolg zijn van een ernstige verstoring van kritieke infrastructuur, zoals gedefinieerd in artikel 2, punt 4), van Richtlijn (EU) 2022/2557[2] van het Europees Parlement en de Raad, wanneer de verstoring of vernietiging van dergelijke kritieke infrastructuur zou leiden tot een imminente dreiging voor het leven of de fysieke veiligheid van een persoon, onder meer door ernstige schade aan de levering van basisvoorzieningen aan de bevolking of aan de uitoefening van de kernfunctie van de staat. Daarnaast moet deze verordening de rechtshandhavingsinstanties en de grenstoezichts-, immigratie- of asielautoriteiten in staat stellen identiteitscontroles uit te voeren in aanwezigheid van de betrokken persoon overeenkomstig de voorwaarden die in het Unierecht

[2] Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (Voor de EER relevante tekst).

Le considérant 33 prévoit que l'utilisation de ces systèmes à des fins répressives devrait donc être interdite, sauf dans des situations précisément répertoriées et rigoureusement définies, dans lesquelles l'utilisation se limite au strict nécessaire à la réalisation d'objectifs d'intérêt général dont l'importance l'emporte sur les risques encourus. Ces situations comprennent la recherche de certaines victimes d'actes criminels, y compris de personnes disparues; certaines menaces pour la vie ou la sécurité physique des personnes physiques, ou des menaces d'attaque terroriste; et la localisation ou l'identification des auteurs ou des suspects des infractions pénales énumérées dans une annexe du présent règlement, lorsque ces infractions pénales sont passibles, dans l'État membre concerné, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins quatre ans et telles qu'elles sont définies dans le droit dudit État membre. Le seuil fixé pour la peine ou la mesure de sûreté privative de liberté prévue par le droit national contribue à garantir que l'infraction soit suffisamment grave pour justifier l'utilisation de systèmes d'identification biométrique à distance "en temps réel". En outre, la liste des infractions pénales figurant en annexe du présent règlement sont basées sur les 32 infractions pénales énumérées dans la décision-cadre 2002/584/JAI du Conseil, compte tenu du fait que certaines de ces infractions sont, en pratique, susceptibles d'être plus pertinentes que d'autres, dans le sens où le recours à l'identification biométrique à distance "en temps réel" pourrait, vraisemblablement, être nécessaire et proportionné, à des degrés très divers, pour les mesures pratiques de localisation ou d'identification d'un auteur ou d'un suspect de l'une des différentes infractions pénales répertoriées, eu égard également aux différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des éventuelles conséquences négatives. Une menace imminente pour la vie ou pour la sécurité physique des personnes physiques pourrait également résulter d'une grave perturbation d'une infrastructure critique, au sens de l'article 2, point 4), de la directive (UE) 2022/2557[2] du Parlement européen et du Conseil, lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie ou la sécurité physique d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice de la fonction essentielle de l'État. Par ailleurs, le présent règlement devrait préserver la capacité des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile d'effectuer des contrôles d'identité en présence de la personne concernée conformément

[2] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (Texte présentant de l'intérêt pour l'EEE).

en het nationale recht voor dergelijke controles zijn vastgelegd. Met name moeten die autoriteiten informatiesystemen kunnen gebruiken in overeenstemming met het Unierecht of het nationale recht om personen te identificeren die tijdens een identiteitscontrole weigeren te worden geïdentificeerd of niet in staat zijn hun identiteit bekend te maken of te bewijzen, zonder dat zij door deze verordening verplicht worden om voorafgaande toestemming te verkrijgen. Het kan hierbij bijvoorbeeld gaan om een persoon die betrokken is bij een misdrijf of iemand die als gevolg van een ongeval of een medische aandoening niet bereid of in staat is zijn identiteit bekend te maken aan rechtshandhavingsinstanties.

Overweging 34 wijst er op dat om ervoor te zorgen dat dergelijke systemen op een verantwoorde en evenredige wijze worden gebruikt, het ook van belang is om vast te stellen dat in elk van die limitatief opgesomde en nauwkeurig omschreven situaties bepaalde elementen in aanmerking moeten worden genomen, met name wat betreft de aard van de situatie die aan het verzoek ten grondslag ligt en de gevolgen van het gebruik voor de rechten en vrijheden van alle betrokken personen, alsook de waarborgen en voorwaarden waaraan het gebruik is onderworpen. Daarnaast mag het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op rechtshandhaving alleen worden ingezet om de identiteit van de specifiek beoogde natuurlijke persoon te bevestigen en moet het worden beperkt tot wat strikt noodzakelijk is qua duur en geografische en personele reikwijdte, met name rekening houdend met het bewijs of de aanwijzingen met betrekking tot de dreigingen, de slachtoffers of de dader. Het gebruik van het systeem voor biometrische identificatie op afstand in real time in openbare ruimten mag alleen worden toegestaan indien de betrokken rechtshandhavingsinstantie een in deze verordening bedoelde effectbeoordeling op het gebied van de grondrechten heeft voltooid en, tenzij anders bepaald in deze verordening, het systeem in de databank heeft geregistreerd zoals vastgelegd in deze verordening. De referentiedatabank van personen moet geschikt zijn voor elk gebruik in elk van de bovenvermelde situaties.

Overweging 35 wijst erop dat voor elk gebruik van een systeem voor biometrische identificatie op afstand in real time in openbare ruimten voor rechtshandhavingsdoeleinden een uitdrukkelijke en specifieke toestemming moet vereist zijn van een gerechtelijke instantie of van een onafhankelijke administratieve instantie van een lidstaat, met bindende beslissingsbevoegdheid. Deze toestemming moet in beginsel worden verkregen voordat het AI-systeem voor de identificatie van een of meer personen wordt gebruikt. Uitzonderingen op

aux conditions prévues par le droit de l'Union et le droit national pour ces contrôles. En particulier, les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile devraient pouvoir utiliser des systèmes d'information, conformément au droit de l'Union ou au droit national, pour identifier une personne qui, lors d'un contrôle d'identité, soit refuse d'être identifiée, soit n'est pas en mesure de décliner son identité ou de la prouver, sans qu'il leur soit fait obligation par le présent règlement d'obtenir une autorisation préalable. Il peut s'agir, par exemple, d'une personne impliquée dans une infraction, qui ne veut pas ou ne peut pas divulguer son identité aux autorités répressives en raison d'un accident ou de son état de santé.

Le considérant 34 prévoit qu'afin de s'assurer que ces systèmes soient utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune des situations précisément répertoriées et rigoureusement définies, certains éléments devraient être pris en considération, notamment en ce qui concerne la nature de la situation donnant lieu à la demande et les conséquences de l'utilisation pour les droits et les libertés de toutes les personnes concernées, ainsi que les garanties et les conditions associées à l'utilisation. En outre, l'utilisation, à des fins répressives, de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public ne devrait être déployée que pour confirmer l'identité de la personne spécifiquement ciblée et elle devrait être limitée au strict nécessaire dans le temps, ainsi que du point de vue de la portée géographique et personnelle, eu égard en particulier aux preuves ou aux indications concernant les menaces, les victimes ou les auteurs. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public ne devrait être autorisée que si l'autorité répressive compétente a réalisé une analyse d'impact sur les droits fondamentaux et, sauf disposition contraire du présent règlement, a enregistré le système dans la base de données prévue par le présent règlement. La base de données de référence des personnes devrait être appropriée pour chaque cas d'utilisation dans chacune des situations mentionnées ci-dessus.

Le considérant 35 point sur le fait que toute utilisation d'un système d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives devrait être subordonnée à l'autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre dont la décision est contraignante. Cette autorisation devrait en principe être obtenue avant l'utilisation du système d'IA en vue d'identifier une ou plusieurs personnes. Des exceptions à cette règle

deze regel moeten worden toegestaan in naar behoren gemotiveerde dringende situaties, namelijk in situaties waarin het wegens de noodzaak om het betrokken AI-systeem te gebruiken, feitelijk en objectief onmogelijk is om vóór het begin van het gebruik toestemming te verkrijgen. In dergelijke dringende situaties moet het gebruik van het AI-systeem worden beperkt tot het absoluut noodzakelijke minimum en onderworpen zijn aan passende waarborgen en voorwaarden, zoals bepaald in de nationale wetgeving en door de rechtshandhavingsinstantie zelf vastgesteld in de context van elk afzonderlijk dringend gebruik. In dergelijke situaties moet de rechtshandhavingsinstantie onverwijld en uiterlijk binnen 24 uur om dergelijke toestemming verzoeken, met opgave van de redenen waarom zij niet eerder een verzoek daartoe heeft kunnen indienen. Indien een dergelijke toestemming wordt geweigerd, moet het gebruik van systemen voor biometrische identificatie in real time waarop dat verzoek betrekking heeft, met onmiddellijke ingang worden stopgezet en moeten alle gegevens met betrekking tot dat gebruik worden verwijderd en gewist. Onder dergelijke gegevens wordt verstaan: inputdata die rechtstreeks door een AI-systeem zijn verkregen tijdens het gebruik van een dergelijk systeem, alsook de resultaten en output van het gebruik in verband met dat verzoek. Daaronder mag niet worden verstaan: input die rechtmatig is verkregen overeenkomstig een ander Unierecht of nationaal recht. In geen geval mag een besluit dat nadelige rechtsgevolgen heeft voor een persoon uitsluitend worden genomen op basis van de output van het systeem voor biometrische identificatie op afstand.

De overweging 36 bepaalt dat om hun taken overeenkomstig de eisen van deze verordening en de nationale regels uit te voeren, de betrokken markttoezichtautoriteit en de nationale gegevensbeschermingsautoriteit moeten in kennis worden gesteld van elk gebruik van het systeem voor biometrische identificatie in real time. De markttoezichtautoriteiten en de nationale gegevensbeschermingsautoriteiten die in kennis zijn gesteld, moeten bij de Commissie een jaarverslag indienen over het gebruik van systemen voor biometrische identificatie in real time.

De overweging 37 bepaalt dat voorts binnen het door deze verordening gestelde limitatieve kader moet worden vastgelegd dat een dergelijk gebruik op het grondgebied van een lidstaat overeenkomstig deze verordening alleen mogelijk mag zijn indien en voor zover de betrokken lidstaat heeft besloten om in zijn specifieke regels van nationaal recht uitdrukkelijk te voorzien in de mogelijkheid om een dergelijk gebruik toe te staan. Bijgevolg staat het de lidstaten uit hoofde van deze verordening vrij in het geheel niet in een dergelijke mogelijkheid te

devraient être autorisées dans des situations dûment justifiées en raison du caractère urgent, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est de nature à rendre effectivement et objectivement impossible l'obtention d'une autorisation avant de commencer à utiliser le système d'IA. Dans de telles situations d'urgence, l'utilisation du système d'IA devrait être limitée au strict nécessaire et assortie de garanties et de conditions appropriées, telles qu'elles sont déterminées dans le droit national et spécifiées dans le contexte de chaque cas d'utilisation urgente par les autorités répressives elles-mêmes. En outre, l'autorité répressive devrait, dans ce genre de situation, solliciter une telle autorisation tout en indiquant les raisons pour lesquelles elle n'a pas été en mesure de le faire plus tôt, sans retard injustifié et au plus tard dans un délai de 24 heures. Lorsqu'une demande d'autorisation est rejetée, l'utilisation de systèmes d'identification biométrique en temps réel liés à cette autorisation devrait cesser immédiatement et toutes les données relatives à cette utilisation devraient être mises au rebut et supprimées. Ces données comprennent les données d'entrée directement acquises par un système d'IA au cours de l'utilisation de ce système, ainsi que les résultats et sorties de l'utilisation liée à cette autorisation. Cela ne devrait pas comprendre les entrées qui sont légalement acquises dans le respect d'un autre droit national ou du droit de l'Union. En tout état de cause, aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne devrait être prise sur la seule base des sorties du système d'identification biométrique à distance.

Le considérant 36 prévoit qu'afin de s'acquitter de leurs tâches conformément aux exigences énoncées dans le présent règlement ainsi que dans les règles nationales, l'autorité de surveillance du marché concernée et l'autorité nationale chargée de la protection des données devraient être informées de chaque utilisation du système d'identification biométrique en temps réel. Les autorités de surveillance du marché et les autorités nationales chargées de la protection des données auxquelles une notification a été adressée devraient présenter à la Commission un rapport annuel sur l'utilisation des systèmes d'identification biométrique en temps réel.

Le considérant 37 prévoit qu'en outre, il convient de prévoir, dans le cadre exhaustif établi par le présent règlement, qu'une telle utilisation sur le territoire d'un État membre conformément au présent règlement ne devrait être possible que dans le cas et dans la mesure où l'État membre concerné a décidé de prévoir expressément la possibilité d'autoriser une telle utilisation dans des règles détaillées de son droit national. Par conséquent, les États membres restent libres, en vertu du présent règlement, de ne pas prévoir une telle possibilité, ou de

voorzien, dan wel slechts in een dergelijke mogelijkheid te voorzien voor een aantal van de in deze verordening genoemde doelstellingen die het toestaan van een dergelijk gebruik rechtvaardigen. Dergelijke nationale regels moeten binnen dertig dagen na de vaststelling ervan ter kennis van de Commissie worden gebracht.

De overweging 38 bepaalt dat het gebruik van AI-systemen voor biometrische identificatie op afstand in real time van natuurlijke personen in openbare ruimten voor rechtshandhavingsdoeleinden noodzakelijkerwijs de verwerking met zich meebrengt van biometrische gegevens. De regels in deze verordening die, met inachtneming van bepaalde uitzonderingen, een dergelijk gebruik verbieden en die gebaseerd zijn op artikel 16 VWEU[3], moeten als *lex specialis* gelden ten aanzien van de regels inzake de verwerking van biometrische gegevens in artikel 10 van Richtlijn (EU) 2016/680[4], waardoor een dergelijk gebruik en de bijbehorende verwerking van biometrische gegevens limitatief worden geregeld. Daarom mogen een dergelijk gebruik en een dergelijke verwerking alleen mogelijk zijn voor zover zij verenigbaar zijn met het bij deze verordening vastgestelde kader, zonder dat er buiten dat kader ruimte is voor de bevoegde autoriteiten om, wanneer zij optreden met het oog op de rechtshandhaving, dergelijke systemen te gebruiken en dergelijke gegevens in verband daarmee te verwerken om de in artikel 10 van Richtlijn (EU) 2016/680 genoemde redenen. In die context is deze verordening niet bedoeld om de rechtsgrondslag te bieden voor de verwerking van persoonsgegevens op grond van artikel 8 van Richtlijn (EU) 2016/680. Het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten voor andere doeleinden dan rechtshandhaving, ook door bevoegde autoriteiten, mag echter niet worden opgenomen in het specifieke kader met betrekking tot dergelijk gebruik voor rechtshandhavingsdoeleinden dat bij deze verordening wordt vastgesteld. Dergelijk gebruik voor andere doeleinden dan rechtshandhaving is derhalve niet onderworpen aan het vereiste van toestemming uit hoofde van deze verordening en de toepasselijke specifieke regels van nationaal recht die aan die toestemming uitvoering kunnen geven.

De overweging 94 bepaalt dat elke vorm van verwerking van biometrische gegevens voor

[3] Verdrag betreffende de werking van de Europese Unie, bekendgemaakt in het *Publicatieblad van de Europese Unie* op 26 oktober 2012, C 326/47.

[4] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

prévoir une telle possibilité uniquement pour certains objectifs parmi ceux susceptibles de justifier l'utilisation autorisée définis dans le présent règlement. Ces règles nationales devraient être notifiées à la Commission dans les 30 jours suivant leur adoption.

Le considérant 38 prévoit que l'utilisation de systèmes d'IA pour l'identification biométrique à distance en temps réel de personnes physiques dans des espaces accessibles au public à des fins répressives passe nécessairement par le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, et qui sont fondées sur l'article 16 du traité sur le fonctionnement de l'Union européenne[3], devraient s'appliquer en tant que *lex specialis* pour ce qui est des règles sur le traitement des données biométriques figurant à l'article 10 de la directive (UE) 2016/680[4], réglementant ainsi de manière exhaustive cette utilisation et le traitement des données biométriques qui en résulte. Par conséquent, une telle utilisation et un tel traitement ne devraient être possibles que dans la mesure où ils sont compatibles avec le cadre fixé par le présent règlement, sans qu'il soit possible pour les autorités compétentes, lorsqu'elles agissent à des fins répressives en dehors de ce cadre, d'utiliser ces systèmes et de traiter ces données pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement ne vise pas à fournir la base juridique pour le traitement des données à caractère personnel en vertu de l'article 8 de la directive (UE) 2016/680. Cependant, l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins autres que répressives, y compris par les autorités compétentes, ne devrait pas être couverte par le cadre spécifique concernant l'utilisation à des fins répressives établi par le présent règlement. L'utilisation à des fins autres que répressives ne devrait donc pas être subordonnée à l'exigence d'une autorisation au titre du présent règlement et des règles détaillées du droit national applicable susceptibles de donner effet à cette autorisation.

Le considérant 94 prévoit que tout traitement de données biométriques intervenant dans l'utilisation de

[3] Traité sur le fonctionnement de l'Union européenne, publiée dans le *Journal officiel de l'Union européenne* du 26 octobre 2012, C326/47.

[4] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

rechtshandhavingsdoeleinden door AI-systemen voor biometrische identificatie, in overeenstemming moet zijn met artikel 10 van Richtlijn (EU) 2016/680, op grond waarvan verwerking uitsluitend is toegestaan indien die strikt noodzakelijk is, in welk geval er passende waarborgen voor de rechten en vrijheden van de betrokkene moeten worden geboden, alsmede indien het Unierecht of het lidstatelijk recht in een dergelijke verwerking voorziet. Een dergelijk gebruik moet, indien toegestaan, tevens voldoen aan de beginselen van artikel 4, lid 1, van Richtlijn (EU) 2016/680, waaronder rechtmatigheid, billijkheid en transparantie, doelbinding, nauwkeurigheid en opslagbeperking.

Artikel 5, lid 3, van de Verordening voorziet dat elk gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving afhankelijk wordt gesteld van een voorafgaande toestemming die wordt verleend door een gerechtelijke instantie of een onafhankelijke administratieve instantie, waarvan het besluit bindend is, van de lidstaat waarin het gebruik moet plaatsvinden en die wordt gegeven op verzoek en in overeenstemming met de gedetailleerde regels van het nationale recht.

Artikel 5, lid 5, en de al vermelde overweging 37 van de Verordening voorzien dat een toegestaan gebruik van een AI-systeem voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving op het grondgebied van een lidstaat, enkel mogelijk is indien en voor zover de betrokken lidstaat heeft besloten om in zijn specifieke regels van nationaal recht uitdrukkelijk hierin te voorzien. De noodzakelijke gedetailleerde regels moeten worden vastgelegd voor het verzoek om en de afgifte en het gebruik van, evenals het toezicht en verslaglegging in verband met, de in artikel 5, lid 3, bedoelde vergunningen. In deze regels wordt ook gespecificeerd voor welke doelstellingen van artikel 5, lid 1, eerste alinea, punt h), en voor welke strafbare feiten als bedoeld in punt h), iii), daarvan de bevoegde autoriteiten deze systemen mogen gebruiken met het oog op de rechtshandhaving.

Dit wetvoorstel beoogt daaraan te beantwoorden door een wettelijke grondslag te bepalen voor het gebruik van dergelijke systemen en de grenzen en de voorwaarden te bepalen van artikel 5, lid 1, eerste alinea, punt h), en de leden 2 tot 4 en 6 van de Verordening.

Zoals hoger vermeld zullen de bepalingen met betrekking tot de verboden AI-praktijken, zoals bepaald in artikel 5 van de Verordening van toepassing zijn met ingang van 2 februari 2025.

Teneinde tijdig en voor die datum te voldoen aan de door de Verordening gestelde vereisten met betrekking tot

systèmes d'IA à des fins d'identification biométrique de nature répressive doit être conforme à l'article 10 de la directive (UE) 2016/680, qui n'autorise un tel traitement que lorsque cela est strictement nécessaire, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre. Une telle utilisation, lorsqu'elle est autorisée, doit également respecter les principes énoncés à l'article 4, paragraphe 1, de la directive (UE) 2016/680, notamment la licéité, la loyauté et la transparence, la limitation des finalités, l'exactitude et la limitation de la conservation.

L'article 5, paragraphe 3, du Règlement prévoit que chaque utilisation à des fins répressives d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public est subordonnée à une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante dont la décision est contraignante de l'État membre dans lequel cette utilisation doit avoir lieu, délivrée sur demande motivée et conformément aux règles détaillées du droit national.

L'article 5, paragraphe 5, et le considérant 37 déjà mentionné du Règlement prévoient que l'utilisation autorisée d'un système d'IA pour l'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives sur le territoire d'un État membre n'est possible que si et dans la mesure où l'État membre concerné a décidé de le prévoir expressément dans ses règles spécifiques de droit national. Les règles détaillées nécessaires à la demande, à la délivrance et à l'exercice des autorisations visées au paragraphe 3, ainsi qu'à la surveillance et à l'établissement de rapports y afférents. Ces règles précisent également pour quels objectifs énumérés à l'article 5, paragraphe 3, premier alinéa, point h), et notamment pour quelles infractions pénales visées au point h), iii), les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives.

La présente proposition de loi vise à y répondre en prévoyant une base légale et de déterminer les limites et les conditions énumérées à l'article 5, paragraphe 1er, premier alinéa, point h), et aux paragraphes 2 à 4 et 6 du Règlement.

Comme mentionné ci-dessus, les dispositions concernant les pratiques interdites en matière d'IA, telles que prévues à l'article 5 du Règlement, s'appliqueront à partir du 2 février 2025.

Afin de se conformer dans les meilleurs délais et avant cette date aux exigences du Règlement concernant

het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving, is een dringend wetgevend optreden vereist.

Er zijn immers strenge sancties in de vorm van hoge geldboetes in geval van niet-naleving van de bepalingen van de Verordening.

Paul Van Tigchelt (Open Vld)

l'utilisation de systèmes d'identification biométrique à distance en temps réel dans les lieux publics à des fins répressives, une action législative urgente est nécessaire.

Il existe en effet des sanctions strictes sous forme d'amendes élevées en cas de non-respect des dispositions du Règlement.

## WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

In Afdeling 1*bis* van Hoofdstuk IV van Boek I van het Wetboek van Strafvordering wordt een artikel 28*novies*/1 ingevoegd, luidende:

"Art. 28*novies*/1.

§ 1. Het gebruik van artificiële intelligentie systemen voor biometrische identificatie op afstand in real time bedoeld in artikel 3, 42), van de Verordening (EU) 2024/1689 in openbare ruimten met het oog op de rechtshandhaving is toegelaten enkel en voor zover een dergelijk gebruik strikt noodzakelijk is voor een van de volgende doelstellingen:

1° het gericht zoeken naar specifieke slachtoffers van ontvoering, mensenhandel of seksuele uitbuiting van mensen, alsook het zoeken naar vermiste personen;

2° het voorkomen van een specifieke, aanzienlijke en imminente dreiging voor het leven of de fysieke veiligheid van natuurlijke personen of een reële en actuele of reële en voorspelbare dreiging van een terroristische aanslag;

3° de lokalisatie of identificatie van een persoon die ervan wordt verdacht een strafbaar feit te hebben gepleegd, ten behoeve van een strafrechtelijk onderzoek of vervolging of tenuitvoerlegging van een straf voor in bijlage II van de Verordening (EU) 2024/1689 artificiële intelligentie genoemde strafbare feiten waarop een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel staat met een maximumduur van ten minste vier jaar.

§ 2. Het gebruik van systemen voor biometrische identificatie op afstand in real time voor de in paragraaf 1 bedoelde doelstellingen wordt ingezet uitsluitend om de specifiek beoogde persoon te identificeren en te lokaliseren en daarbij wordt rekening gehouden met het volgende:

1° de aard van de situatie die aanleiding geeft tot het mogelijke gebruik van het systeem, met inbegrip van

## PROPOSITION DE LOI

Artikel 1er

La présente proposition règle une matière visée à l'article 74 de la Constitution.

Art. 2

Dans la Section 1*bis* du Chapitre IV du Livre 1er du Code d'instruction criminelle, il est inséré un article 28*novies*/1, rédigé comme suit:

"Art. 28*novies*/1.

§ 1er. L'utilisation de systèmes d'intelligence artificielle d'identification biométrique à distance en temps réel visés par l'article 3, 42), du Règlement (UE) 2024/1689 dans des espaces accessibles au public à des fins répressives est permise uniquement si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs suivants:

1° la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues;

2° la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste;

3° la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II du Règlement (UE) 2024/1689 sur l'intelligence artificielle et punissables d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans.

§ 2. L'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1er, n'est déployée que pour identifier et localiser la personne spécifiquement ciblée et tient compte des éléments suivants:

1° la nature de la situation donnant lieu à un éventuel recours au système, en particulier la gravité, la probabilité

de ernst, waarschijnlijkheid en omvang van de schade die zonder het gebruik van het systeem zou worden veroorzaakt;

2° de gevolgen van het gebruik van het systeem voor de rechten en vrijheden van alle betrokken personen, en met name de ernst, waarschijnlijkheid en omvang van deze gevolgen.

Daarnaast moet het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving voor de in paragraaf 1 genoemde doelstellingen in overeenstemming zijn met noodzakelijke en evenredige waarborgen en voorwaarden in verband met het gebruik overeenkomstig dit artikel. Het gebruik van dergelijke systemen in het kader van bijzondere opsporingsmethoden of andere onderzoeksmethoden is enkel toegestaan indien voldaan is aan de waarborgen en voorwaarden van dit artikel en van de artikelen met betrekking tot die opsporingshandelingen.

Het gebruik van een systeem voor biometrische identificatie op afstand in real time in openbare ruimten wordt alleen toegestaan indien een in artikel 27 van de Verordening (EU) 2024/1689 artificiële intelligentie voorziene effectbeoordeling op het gebied van de grondrechten is uitgevoerd en het systeem volgens artikel 49 van dezelfde Verordening in de EU-databank is geregistreerd. In naar behoren gemotiveerde spoedeisende gevallen kan echter met het gebruik van dergelijke systemen worden begonnen zonder de systemen in de EU-databank te registreren, op voorwaarde dat die registratie zonder onnodige vertraging wordt voltooid.

§ 3. Het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten moet door de procureur des Konings worden gemachtigd.

In een naar behoren gemotiveerde spoedeisende situatie kan echter zonder toestemming met het gebruik van een dergelijk systeem worden begonnen, op voorwaarde dat een dergelijke toestemming zonder onnodige vertraging en ten minste binnen vierentwintig uur wordt aangevraagd. Bij weigering van die toestemming wordt het gebruik onmiddellijk gestaakt en worden alle gegevens, resultaten en outputs van dat gebruik onmiddellijk verwijderd en gewist.

De procureur des Konings verleent de toestemming slechts wanneer hij op basis van objectieve elementen of ernstige aanwijzingen die hem zijn voorgelegd ervan overtuigd is dat het gebruik van het betreffende systeem voor biometrische identificatie op afstand in real time

et l'ampleur du préjudice qui serait causé si le système n'était pas utilisé;

2° les conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences.

En outre, l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1er, respecte les garanties et conditions nécessaires et proportionnées en ce qui concerne cette utilisation, conformément à cet article. L'utilisation de tels systèmes dans le cadre de méthodes particulières de recherche ou d'autres mesures d'enquête n'est autorisée que si les garanties et conditions énoncées dans le présent article et dans les articles relatifs aux mesures d'enquête dans le cadre desquelles ces systèmes sont appliqués sont remplies.

L'utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public n'est autorisée que si une analyse d'impact sur les droits fondamentaux conformément à l'article 27 du Règlement (UE) 2024/1689 sur l'intelligence artificielle a été réalisé et que le système a été enregistré dans la base de données de l'UE prévue par l'article 49 du même Règlement. Toutefois, dans des cas d'urgence dûment justifiés, il est possible de commencer à utiliser ces systèmes sans enregistrement dans la base de données de l'UE, à condition que cet enregistrement soit effectué sans retard injustifié.

§ 3. L'utilisation de systèmes d'intelligence artificielle d'identification biométrique à distance en temps réel dans des espaces accessibles au public doit être autorisée par le procureur du Roi.

Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser ce système sans autorisation à condition que cette autorisation soit demandée sans retard injustifié, au plus tard dans les vingt-quatre heures. Si cette autorisation est rejetée, il est mis fin à l'utilisation avec effet immédiat, et toutes les données, ainsi que les résultats et sorties de cette utilisation, sont immédiatement mis au rebut et supprimés.

Le procureur du Roi accorde l'autorisation uniquement s'il estime, sur la base des éléments objectifs ou des indices sérieux qui lui sont présentés, que l'utilisation du système d'identification biométrique à distance en temps réel concerné est nécessaire et proportionnée

noodzakelijk is voor en evenredig is aan het bereiken van een van de in paragraaf 1 gespecificeerde doelstellingen, zoals genoemd in het verzoek en met name beperkt blijft tot wat strikt noodzakelijk is met betrekking tot de periode en de geografische en personele werkingssfeer. Bij zijn beslissing houdt hij rekening met de in paragraaf 2 bedoelde elementen. Een beslissing die nadelige rechtsgevolgen heeft voor een persoon mag niet uitsluitend worden genomen op basis van de output van het systeem voor biometrische identificatie op afstand in real time.

§ 4. De in paragraaf 3 voorziene machtiging is schriftelijk en vermeldt:

1° de toelating tot het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten;

2° het met het gebruik van deze systemen nagestreefde doel, overeenkomstig paragraaf 1;

3° de periode tijdens welke deze systemen kunnen worden gebruikt en die niet langer mag zijn dan drie maanden te rekenen van de datum van de machtiging;

4° de naam en de hoedanigheid van de officier van gerechtelijke politie, die de leiding heeft over het gebruik van deze systemen;

5° de naam of, indien deze niet bekend is, een zo nauwkeurig mogelijke omschrijving van de persoon of beoogde personen en van de plaatsen of gebeurtenissen bedoeld in paragraaf 1.

§ 5. De procureur des Konings kan steeds op gemotiveerde wijze de machtiging wijzigen, aanvullen of verlengen. Hij kan te allen tijde zijn machtiging intrekken. Hij gaat bij elke wijziging, aanvulling of verlenging van zijn machtiging na of de voorwaarden voor het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten zijn vervuld en handelt overeenkomstig paragraaf 4, 1° tot 5°.

§ 6. De procureur des Konings staat in voor de permanente controle over de toepassing van de systemen voor biometrische identificatie op afstand in real time in openbare ruimten door de politiediensten binnen zijn gerechtelijk arrondissement.

§ 7. Elk gebruik van een systeem voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving wordt gemeld aan de door de Koning daartoe aangewezen nationale markttoezichtautoriteiten en nationale gegevensbeschermingsautoriteiten, die overeenkomstig artikel 5,

à la réalisation de l'un des objectifs énumérés au paragraphe 1er, tels qu'indiqués dans la demande et, en particulier, que cette utilisation reste limitée au strict nécessaire dans le temps et du point de vue de la portée géographique et personnelle. Dans sa décision, il tient compte des éléments visés au paragraphe 2. Aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne peut être prise sur la seule base de la sortie du système d'identification biométrique à distance en temps réel.

§ 4. L'autorisation prévue au paragraphe 3 est délivrée par écrit et précise:

1° l'autorisation d'utiliser des systèmes d'identification biométrique à distance en temps réel dans les lieux publics;

2° l'objectif poursuivi par l'utilisation de ces systèmes, conformément au paragraphe 1er;

3° la période pendant laquelle ces systèmes peuvent être utilisés, qui ne peut excéder trois mois à compter de la date de l'autorisation;

4° le nom et la qualité de l'officier de police judiciaire chargé de l'utilisation de ces systèmes;

5° le nom ou, s'il n'est pas connu, une description aussi précise que possible de la ou des personnes ciblées, ainsi que des lieux ou des événements visés au paragraphe 1er.

§ 5. Le procureur du Roi peut à tout instant, de manière motivée, modifier, compléter ou prolonger l'autorisation. Il peut à tout moment retirer son autorisation. Il vérifie si les conditions d'utilisation des systèmes d'identification biométrique en temps réel à distance dans les lieux publics sont remplies chaque fois que son autorisation est modifiée, complétée ou prolongée et agit conformément au paragraphe 4, 1° à 5°.

§ 6. Le procureur du Roi exerce un contrôle permanent sur la mise en œuvre des systèmes d'identification biométrique en temps réel à distance dans les lieux publics par les services de police au sein de son arrondissement judiciaire.

§ 7. Toute utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives est notifiée aux autorités nationales de surveillance du marché et aux autorités nationales chargées de la protection des données, désignées à cet effet par le Roi, qui soumettent

lid 6, van de Verordening (EU) 2024/1689 artificiële intelligentie een jaarlijks verslag indienen bij de Europese Commissie. Deze melding bevat geen gevoelige operationele gegevens."

11 december 2024

Paul Van Tigchelt (Open Vld)

un rapport annuel à la Commission européenne, conformément à l'article 5, paragraphe 6, du Règlement (UE) 2024/1689 sur l'intelligence artificielle. Cette notification ne contient pas de données opérationnelles sensibles."

11 décembre 2024



Centrale drukkerij - Imprimerie centrale