



> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018 2500
EA DEN HAAG

**Directoraat-Generaal
Politie en
Veiligheidsregio's**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
3175535

Uw kenmerk
2020Z24391

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

19 januari 2021

Onderwerp Antwoorden kamervragen over het bericht 'We gaan niet de hele dag
meekijken'

In antwoord op uw brief van 9 december 2020 deel ik u mee dat de schriftelijke
vragen van het lid Van Dam (CDA) over het bericht 'We gaan niet de hele dag
meekijken', worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Justitie en Veiligheid,

1Pagina1van2

Ferd Grapperhaus

Antwoorden van de minister van Justitie en Veiligheid op schriftelijke vragen van het lid Van Dam (CDA) over het bericht 'We gaan niet de hele dag meekijken' (ingezonden 9 december 2020, 2020Z24391)

Directoraat-Generaal
Politie en
Veiligheidsregio's

Datum
11 januari 2021

Ons kenmerk 3175535

Vraag 1

Bent u bekend met het bericht 'We gaan niet de hele dag meekijken'? 1)

Antwoord op vraag 1

Ja.

Vraag 2

Kunt u - op hoofdlijnen - aangeven op welke wijze politiemedewerkers met toegang tot de politiesystemen gecontroleerd gaan worden om te zien of ze geen vreemd zoekgedrag vertonen? Kunt u daarbij duiden op welke wijze opvolging wordt gegeven aan afwijkende signalen en op welke wijze 'het gesprek met de medewerker' ingebed is in de vervolgaanpak?

Vraag 3

Wat zijn atypische signalen waarop vreemd zoekgedrag geconstateerd gaat worden precies? Kunt u dit nader duiden?

Antwoorden op vragen 2 en 3

Burgers mogen ervan uitgaan dat informatie die bij de politie bekend is uiterst zorgvuldig wordt behandeld en beschermd. Het lekken van informatie brengt naast de inbreuk op de privacy van de betrokkene mogelijk ook de veiligheid van operaties en mensen in gevaar. De politie gaat daarom oneigenlijk gebruik van de politiesystemen sneller detecteren met de bedoeling deze eerder te stoppen. Recente corruptiezaken onderstrepen het belang van verscherpte aandacht voor de aanpak van het lekken van informatie.

Daartoe is een systeem en werkwijze in ontwikkeling met als doel om in een vroegtijdig stadium mogelijk misbruik door gericht binnendringen van de politiesystemen (*hacken*) en lekken van informatie van binnenuit te detecteren en voorkomen. Het systeem geeft een indicatie of mogelijk sprake is van afwijkend zoekgedrag op basis van een groot aantal indicatoren, waaronder het historische patroon van bevraging en een vergelijking met het gemiddelde bevragingspatroon van collega's. Deze indicatoren zijn gebaseerd op input en ervaringen van experts binnen de politieorganisatie plus de analyse van casuïstiek. Een voorbeeld van een indicator is het doen van bevragingen met betrekking tot een onderzoek waar de betreffende functionaris geen rol in heeft. Het is belangrijk om op te merken dat 'afwijkend zoekgedrag' niet perse 'fout gedrag' hoeft te betekenen. Om te zorgen dat er geen sprake is van automatische besluitvorming en er altijd een mens meekijkt en beslist, wordt een indicatie door specialisten geanalyseerd en gewogen. Als er vervolgens aanleiding is tot verdere actie wordt de indicatie besproken met de leidinggevende die een nadere afweging maakt voor het vervolg. In de gevallen dat sprake is van een harde verdenking van bijvoorbeeld corruptie in relatie tot georganiseerde criminaliteit wordt uiteraard een passende aanpak gekozen.

De gehele aanpak is op dit moment nog in ontwikkeling en het perspectief van medewerkers speelt daarbij een belangrijke rol. De medezeggenschap is akkoord

gegaan met de ontwikkelingsfase, neemt vanaf de start deel aan de begeleidingsgroep en stuurgroep en zal bij de landelijke inrichting en uitrol om instemming worden gevraagd. Het ondersteunen van alle integere politiemedewerkers en het belang van hun vertrouwen wordt nadrukkelijk onderkend.

**Directoraat-Generaal
Politie en
Veiligheidsregio's**

Datum
11 januari 2021

Ons kenmerk3175535

Vraag 4

Kunt u uitleggen hoe het juridisch raamwerk van dit systeem precies in elkaar zit? Is het een werkgever toegestaan om het zoekgedrag van medewerkers op deze manier te monitoren?

Antwoord op vraag 4

De verwerking van informatie door de politie wordt uitgevoerd binnen de wettelijke kaders van de Wet politiegegevens (WPG). Artikel 3 WPG vereist dat politiegegevens slechts worden verwerkt voor zover dit behoorlijk en rechtmatig is. Door middel van het actief loggen van de verwerking van politiegegevens kan de rechtmatigheid van de verwerking worden gecontroleerd. Het bijhouden en beoordelen daarvan volgt daarnaast uit artikel 4a WPG. Daarin is geregeld dat de politie passende technische en organisatorische maatregelen moet treffen om een passend beveiligingsniveau te waarborgen. Deze zogenaamde verplichting tot informatiebeveiliging vereist dat "logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig worden beoordeeld". De Autoriteit Persoonsgegevens heeft daarbij duidelijk aangegeven, dat deze (impliciete) monitoringsverplichting niet alleen achteraf geldt. Ook moeten de logbestanden proactief gecontroleerd worden op indicaties van onrechtmatige toegang of onregelmatig gebruik van politiegegevens. Om logbestanden te kunnen monitoren of beoordelen is het nodig om vooraf indicaties vast te stellen waarop deze beoordeling kan plaatsvinden.

In de WPG is tevens een expliciete verplichting voor de politie opgenomen om langs elektronische weg een aantal verwerkingen van politiegegevens in geautomatiseerde systemen vast te leggen (artikel 32a WPG). Deze verplichting tot logging vloeit voort uit EU richtlijn 2016/680 betreffende de gegevensbescherming inzake opsporing en vervolging. De logbestanden mogen uitsluitend worden gebruikt om te controleren of de gegevensverwerking rechtmatig is, om interne controle uit te oefenen, om de integriteit en de beveiliging van de gegevens te garanderen en om strafrechtelijke procedures te waarborgen. Hierbij omvat interne controle mede het voeren van interne tuchtprocedures.

Op basis van het gegevensbeschermingsrecht is het dus toegestaan, en zelfs verplicht dat dergelijke handelingen van politiemedewerkers worden gelogd en gemonitord.

De verplichting tot logging van artikel 32a WPG is nog niet in werking getreden. De EU richtlijn biedt de mogelijkheid tot uitstel van inwerkingtreding tot 2023. Dit geeft de politie ruimte en tijd om de ICT-systemen geleidelijk aan te passen.

Vraag 5

Klopt het dat de MEOS-applicatie (MobiEl Effectief Op Straat) voor iedere operationele politieman beschikbaar is, inclusief aspiranten van politie vanaf hun eerste werkdag? Klopt het dat MEOS voor iedere individuele politieman 24 uur per dag beschikbaar is, 365 dagen per jaar? Klopt het

dat MEOS door iedere politieman overal ter wereld (waar een internetaansluiting is) te raadplegen is?

**Directoraat-Generaal
Politie en
Veiligheidsregio's**

Antwoord op vraag 5

De MEOS-applicatie is voor operationele doeleinden altijd en overal beschikbaar voor alle medewerkers in de operatie; hieronder vallen ook aspiranten die immers als onderdeel van hun opleiding ook ingezet worden op straat en daartoe worden toegerust met onder andere de MEOS-applicatie en zo de noodzakelijke ervaring hiermee opdoen. In het nieuwe politieonderwijs (PO 21) zijn aspiranten in het eerste jaar meer op school en zullen zij door middel van een speciale oefenomgeving –die op dit moment ontwikkeld wordt- zich bekwamen in het gebruik van het MEOS-systeem. Technisch bestaat de mogelijkheid MEOS te raadplegen in het buitenland, maar dit is uiteraard alleen geoorloofd als het om het operationeel belang gaat. Het is niet toegestaan politie informatie voor andere doeleinden dan de operationele taak te gebruiken.

Datum
11 januari 2021

Ons kenmerk3175535

Vraag 6

Op welke wijze kan een politieman die zich oprecht zorgen maakt over een omstandigheid op de grens van werk en privé op een fatsoenlijke en rechtmatige wijze gebruik maken van informatie uit politiesystemen?

Kunt u de beantwoording van deze casus toespitsen op 2 specifieke situaties: (1) er komen nieuwe burens waarbij de betrokken politieambtenaar in ernstige mate twijfelt of het aangaan van een normale burenrelatie zich verhoudt tot een integere beroepsuitoefening en (2) een familielid van de politieambtenaar gaat een relatie aan met een persoon die in zijn gedrag tekenen van een actieve criminele loopbaan laat zien?

Antwoord op vraag 6

Zoals ik hiervoor al heb aangegeven is het niet toegestaan politie informatie voor andere doeleinden dan de operationele taak te gebruiken. Als een politiefunctionaris in persoon, via een familielid of een andere nauwe relatie betrokken is bij een bepaalde situatie die op zichzelf aanleiding geeft tot het raadplegen van politiesystemen, dan moet deze functionaris die situatie bespreken met zijn leidinggevende. In veel van dergelijke situaties bestaat overigens per definitie de noodzaak om het eventuele veiligheidsrisico te melden bij de leidinggevende.

1) NRC, 7 december 2020, 'We gaan niet de hele dag meekijken',
<https://www.nrc.nl/nieuws/2020/12/07/we-gaan-niet-de-hele-dag-meekijken-a4022930>