

Privacy en Veiligheid

Opereren in het spanningsveld

Hoe ga je als bestuurder om met gevoelige informatie in een wereld van toenemende digitale dreigingen? Tijdens het tweede bestuurlijk mini-symposium van het Centrum voor Veiligheid en Digitalisering (CVD) in Apeldoorn verkenden bestuurders, toezichthouders, politie, private partijen en onderzoekers gezamenlijk het spanningsveld tussen privacy, veiligheid en samenwerking. Geen makkelijke opgave, zo benadrukte CVD-bestuurder en dagvoorzitter Maarten van Steen: “Als er een directe oplossing was, dan was het geen dilemma.”

Ton Heerts: “De praktijk weet het CVD goed te vinden”

Burgemeester van Apeldoorn en mede-initiatiefnemer van het CVD, Ton Heerts, opende het symposium met de observatie dat “de praktijk het CVD goed weet te vinden.” Bij het Centrum voor Veiligheid en Digitalisering komen verschillende vraagstukken voorbij: van datalekken en ethische dilemma’s tot hoe om te gaan met onlinegedrag of informatie-uitwisseling in complexe ketens. Ton Heerts benadrukte dat het CVD er juist is om die casuïstiek niet vanuit één organisatie of discipline te benaderen, maar in gezamenlijkheid. Vragen worden niet alleen juridisch of technisch bekeken, maar besproken met mensen uit de praktijk, bestuurders en toezichthouders.





Over kaders en keuzes, keynote door Aleid Wolfsen

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens (AP), gaf in zijn keynote een overzicht van de juridische kaders rond het verwerken van persoonsgegevens. Zijn boodschap: gegevensverwerking is niet zomaar een technische handeling, maar raakt direct aan het recht op privacy.

*“Als je persoonsgegevens verwerkt,
meng je je in een grondrecht. Punt.”*

Aleid Wolfsen, Autoriteit Persoonsgegevens

De AVG (Algemene Verordening Gegevensbescherming) werkt dit Europese grondrecht concreet uit en bepaalt hoe persoonsgegevens verzameld, gebruikt en gedeeld mogen worden. Daarbij geldt een duidelijke volgorde: het EU-Handvest staat boven de AVG, en de AVG weer boven nationale wetgeving zoals de Nederlandse Grondwet.

Volgens Wolfsen moeten persoonsgegevens dan ook niet als vrij beschikbaar worden gezien. Een eenvoudige vergelijking maakt dat duidelijk: “Je mag een fiets die ergens buiten staat ook niet zomaar meenemen.” Zo werkt het met data ook, alleen op een wettelijke basis of expliciete toestemming.

Voor bijzondere persoonsgegevens, zoals medische gegevens of informatie over religie of politieke voorkeur, gelden strengere eisen. Maar ook bij gewone gegevens moet elke verwerking doelgericht en transparant zijn. Wolfsen benadrukte dat het helpt om goed uit te leggen waarom iets wordt gedaan: “Dan kom je vaak al een heel eind.”





Aleid Wolfsen stond niet alleen stil bij de regels, maar kwam ook met praktijkvoorbeelden waarbij het misging. Zowel in de toeslagenaffaire als bij de controles door DUO bleken algoritmes mensen te benadelen op basis van kenmerken als nationaliteit, leeftijd of opleidingsniveau. Persoonsgegevens dus. Zo werden bij DUO jarenlang mbo-studenten met een migratieachtergrond vaker gecontroleerd, dat gebeurde op basis van data en persoonsgegevens die in een algoritme werden verwerkt, zonder besef dat dit in strijd was met de wet.

Om onder andere dit soort situaties te voorkomen is de rol van Functionaris Gegevensbescherming (FG) in het leven geroepen. Deze professionals hebben een onafhankelijke rol en vormen de eerste interne waarborg tegen risicovolle of onrechtmatige gegevensverwerking. Voor de AP zijn zij dan ook bondgenoten in de bescherming van grondrechten én waardevolle gesprekspartners. Zij kunnen op elk moment, 24/7, rekenen op steun, advies of toetsing van de AP.

Wolfsen sloot af met de oproep om FG's eerder te betrekken bij strategische en ethische afwegingen: wat mag er, wat kan er en wat past bij de waarden van de organisatie? Door hier tijdig over in gesprek te gaan benut je de juridische ruimte die er wél is.

*“Grondrechten zijn er niet om innovatie of veiligheid te blokkeren,
maar om onze samenleving te beschermen tegen willekeur.
Vooral in het digitale domein.”*

Aleid Wolfsen, Autoriteit Persoonsgegevens

Paneldiscussie: balanceren tussen privacy, veiligheid en actie

In de daaropvolgende paneldiscussie werd duidelijk hoe veelzijdig de vraagstukken rond gegevensdeling zijn. Juridische regels geven richting, maar botsen soms met snelle technologische ontwikkelingen of maatschappelijke verwachtingen.



Ben den Tuinder, juridisch docent en onderzoeker bij het lectoraat Weerbare Democratie van Hogeschool Saxion, pleitte voor bestuurders die niet alleen kijken naar wat wettelijk mag, maar ook naar wat ethisch passend is. “Waarden wijzen de weg waar regels eindigen,” stelde hij. Afspraken over gegevensuitwisseling zijn vaak gestoeld op de technologische inzichten van dat moment, en mogen volgens hem regelmatig herijkt worden.

Samen met andere consortiumpartners onderzoekt Ben vanuit het lectoraat hij hoe publieke organisaties in de schuldhulpverlening proactief contact kunnen leggen met burgers, zonder hun autonomie, privacy of vertrouwen te schaden. Een rapport hierover verschijnt eind dit jaar.

Liesbeth Holterman van Cyberveilig Nederland wees op het belang van tempo en vertrouwen in de samenwerking tussen de private sector en overheden. Nieuwe regels zoals NIS2 en de AI-verordening leiden tot een sterke focus op naleving, waardoor noodzakelijke informatiedeling soms blijft liggen. Toch ziet zij ruimte bij toezichthouders, zoals de AP, om samen te kijken wat wel kan. In het samenwerkingsverband ‘Melissa’ wordt bijvoorbeeld al operationele informatie gedeeld tussen publieke en private partijen. Haar voorstel: ontwikkel zogeheten ‘fast tracks’ in afgebakende omgevingen, zodat ook in urgente situaties snel én verantwoord informatie kan worden gedeeld.



Anne-Jan Oosterheert, hoofd Operatiën Politie Oost-Nederland en daarnaast voor de politie landelijk portefeuillehouder aanpak digitale criminaliteit, schetste het beeld van een groeiende digitale dreiging. Volgens hem kunnen publieke instanties dit probleem niet alleen oplossen. “We zitten in een hybride ‘oorlogsomgeving’, dan heb je elkaar nodig.” Met een individuele aanpak gaan we de strijd niet winnen. We hebben het bedrijfsleven nodig, bijvoorbeeld voor het signaleren van cyberaanvallen. Toch merkt hij dat veel publieke instanties terughoudend zijn om deze data te delen, vooral uit angst om de regels te overtreden. Die onzekerheid belemmert samenwerking, terwijl snelle en zorgvuldige informatie-uitwisseling essentieel is om Nederland digitaal veilig te houden.

Henriëtte Bongers van de Fraudehelpdesk bracht het perspectief van burgers in. De helpdesk ontvangt dagelijks meldingen van online fraude, maar mag geen dadergegevens verwerken of bewaren. Toch wees zij op een recent experiment dat erg succesvol is gebleken. Bij dit experiment werd een politiemedewerker betrokken en met toestemming van de melder werden gegevens gericht doorgestuurd, wat leidde tot meer aangiftes, tevreden melders en effectievere vervolgstappen. Zo’n voorbeeld laat volgens haar zien dat samenwerking binnen duidelijke afspraken wel degelijk kan.





Wat alle sprekers deelden, was het idee dat verantwoord gegevens delen niet vanzelf gaat, maar wel mogelijk is. Mits er ruimte is voor maatwerk, wederzijds begrip en een gezamenlijke wil om te zoeken naar wat wél kan.

Niet alles kan, maar wel meer dan je denkt

De gesprekken lieten zien dat het delen van informatie tussen partijen vraagt om heldere afspraken en onderling vertrouwen. Er is zelden een pasklare route, maar door elkaar op te zoeken en open te blijven kijken naar mogelijkheden binnen bestaande kaders, ontstaat wél ruimte. Niet alles kan, maar er blijkt vaak meer mogelijk dan gedacht.



Centrum voor
Veiligheid en
Digitalisering