

Commissie voor Justitie

van

WOENSDAG 24 SEPTEMBER 2025

Namiddag

Commission de la Justice

du

MERCREDI 24 SEPTEMBRE 2025

Après-midi

La réunion publique de commission est ouverte à 13 h 31 et présidée par M. Ismaël Nuino.  
De openbare commissievergadering wordt geopend om 13.31 uur en voorgezeten door de heer Ismaël Nuino.

*Les textes figurant en italique dans le Compte rendu intégral n'ont pas été prononcés et sont la reproduction exacte des textes déposés par les auteurs.*

*De teksten die cursief zijn opgenomen in het Integraal Verslag werden niet uitgesproken en steunen uitsluitend op de tekst die de spreker heeft ingediend.*

**01** Question de Patrick Prévot à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le mode sentinelle des voitures Tesla" (56007043C)

**01** Vraag van Patrick Prévot aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De waakmodus van Tesla's" (56007043C)

**01.01** Patrick Prévot (PS): Madame la ministre, bien que les achats de véhicules Tesla soient en chute libre en Belgique, notamment pour des raisons géopolitiques et en réaction aux frasques de son PDG Elon Musk, il n'en reste pas moins que près de 21 000 Tesla sont immatriculées en Belgique. L'une des fonctionnalités de ces véhicules pose problème pour la protection de la vie privée et constitue une infraction au regard du Règlement général sur la protection des données (RGPD). Je veux parler ici du "mode Sentinelle".

Pour résumer, même lorsqu'elles sont stationnées, les caméras extérieures de la voiture continuent à tourner. Or, il est interdit de filmer l'espace public. Le concessionnaire Tesla ou le propriétaire d'une Tesla serait dans l'obligation d'afficher un pictogramme prévenant les personnes qu'elles seraient susceptibles d'être filmées – un pictogramme que nous voyons collé sur extrêmement peu de véhicules. Or, sans ce pictogramme, le ou la propriétaire s'expose à des amendes qui peuvent aller jusqu'à 20 millions d'euros. Dans la pratique, les amendes sont très rares.

En dehors de ces violations au RGPD se pose aussi la question de l'accès aux images enregistrées: sont-elles limitées aux propriétaires ou peuvent-elles remonter jusqu'au siège de Tesla? À ce sujet, je suis effaré d'apprendre que l'entreprise précise que seules les images filmées à l'intérieur de l'habitacle ne lui sont pas transmises. Pour les caméras extérieures utilisées en mode Sentinelle, Tesla affirme laisser le choix à ses clients de partager ou non leurs données (dont les séquences vidéo) avec l'entreprise qui ne les utiliserait que pour améliorer ses services.

Chaque véhicule Tesla est une potentielle caméra de surveillance pour une entreprise étrangère dont le PDG s'est vu être le bras droit de Trump, dans une forme d'hybridation public-privé qui doit évidemment attirer toute notre attention. Nous ne pouvons pas laisser ces faits sans réponse.

Madame la ministre, pourrais-je connaître votre retour sur ce mode Sentinelle actif dans les véhicules Tesla? Confirmez-vous que cette fonctionnalité viole plusieurs législations, à commencer par le RGPD?

**01.02** Vanessa Matz, ministre: Monsieur Prévot, je vous remercie vivement d'avoir attiré une fois de plus notre attention sur des préoccupations effectivement très importantes au regard de la protection de la vie privée.

La question du mode Sentinelle des voitures Tesla n'est pas anodine. Comme vous venez de le dire,

elle soulève à juste titre des préoccupations majeures en matière de protection de la vie privée et de respect du cadre légal. Dans une société numérique où les caméras se multiplient, il est essentiel de fixer des limites claires pour garantir les droits fondamentaux des citoyens. Le droit européen rappelé par la Cour de justice de l'Union européenne (CJUE) est clair: l'utilisation de caméras de surveillance par des particuliers ne peut être tolérée que si elle répond à un intérêt légitime dans des conditions strictes de nécessité et de proportionnalité. En Belgique, cette évaluation relève de l'Autorité de protection des données (APD) qui reçoit déjà des plaintes à ce sujet.

Mais au-delà du Règlement général sur la protection des données, la loi belge est explicite. La loi caméras de 2007 interdit aux particuliers de filmer l'espace public. L'usage actuel du mode Sentinelle contrevient donc à cette loi et les images ainsi collectées ne peuvent être légalement transmises qu'aux forces de l'ordre et au parquet.

La technologie ne peut pas avancer au détriment des droits fondamentaux. Il convient de rester ferme pour garantir la protection de la vie privée de tous les citoyens. C'est pour cette raison et parce que la loi caméras relève des compétences de mon collègue, le ministre de l'Intérieur, que je l'ai concerté pour évaluer les images qui sont filmées par Tesla et déterminer si ce mode Sentinelle est en contradiction, comme je le pense, ou pas avec la loi caméras. Nous allons donc nous concerter à ce sujet pour agir de manière juste par rapport à ce qui me semble être non seulement une infraction aux règles européennes mais aussi au droit national.

**01.03 Patrick Prévot (PS):** Je vous remercie pour votre réponse, madame la ministre.

Effectivement, j'estime qu'il s'agit d'un sujet important au regard de la protection de la vie privée. De plus, ce mode Sentinelle, à titre personnel, me pose question. Cela reste mon problème même si, comme vous l'aurez compris, je n'ai pas de Tesla.

Vous dites que l'APD est claire, et que notre loi nationale est explicite, notamment avec cette loi caméras de 2007 qui interdit l'utilisation de caméras dans l'espace public. Je suis donc content d'entendre que vous avez interpellé votre collègue, le ministre de l'Intérieur, pour évaluer si ce mode Sentinelle est en contradiction avec la loi caméras. C'est le cas, selon vous. Je partage votre position, mais il s'agit bien de votre interprétation. Cela me porte à croire que, parmi ce duo du ministre de l'Intérieur et vous-même, une des deux parties partage mon sentiment. Je ne doute pas que vous prendrez les mesures qui s'imposent si jamais vos avis convergent, et que ce mode Sentinelle est en infraction avec les règles européennes ou avec la législation nationale.

*Het incident is gesloten.*

*L'incident est clos.*

**02 Vraag van Dieter Keuten aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "Het risico op een datalek bij een bevolkingsonderzoek" (56007664C)**

**02 Question de Dieter Keuten à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le risque d'une fuite de données lors d'un dépistage de la population" (56007664C)**

**02.01 Dieter Keuten (VB):** Mevrouw de minister, in Nederland was er een datalek bij een laboratorium dat verantwoordelijk is voor een bevolkingsonderzoek naar baarmoederhalskanker. Zeer gevoelige persoonsgegevens, in casu medische gegevens, namen, adressen, testuitslagen van deelnemers en zelfs rijksregisternummers werden gestolen. De gestolen gegevens maken diverse vormen van misbruik door hackers mogelijk. Ongeveer 850.000 Nederlanders werden getroffen en inmiddels hebben 68.000 vrouwen zich gemeld voor een gezamenlijke schadeclaim. Niet alleen doet die zaak de wenkbrauwen fronsen, ze wekt ook de vrees voor een herhaling ervan in België.

Mevrouw de minister, kan zo'n datalek ook in België gebeuren? Welke garanties bieden Belgische overheidsdiensten onze burgers in verband met de opslag van hun persoonlijke gegevens? Welke beveiligingsmaatregelen gelden ten opzichte van externe organisaties die bijvoorbeeld bevolkingsonderzoeken organiseren? Hebt u hierover overleg gehad met bijvoorbeeld de data protection officer van het Belgische federale eHealth-platform?

**02.02** Minister **Vanessa Matz**: Mijnheer Keuten, het recente datalek in Nederland toont opnieuw aan dat de bescherming van persoonlijke gegevens een grote uitdaging blijft. Het gaat niet alleen om de privacy van burgers, maar ook om hun vertrouwen in onze instellingen. Elke nalatigheid is onaanvaardbaar. In België geldt een sterk wettelijk kader. De AVG verplicht organisaties om gegevens te beveiligen. Een datalek moet binnen 72 uur worden gemeld aan de Gegevensbeschermingsautoriteit en de betrokkenen moeten geïnformeerd worden, indien er sprake is van een risico. De GBA ziet hierop toe en kan sancties opleggen.

Het incident toont aan dat cyberveiligheid geen luxe is, maar een noodzaak. Zowel de overheid als de betrokken organisaties moeten hun praktijken versterken. Ik heb de administratie opgedragen de privacywetgeving te evalueren en, indien nodig, in overleg met de sectoren aan te passen.

Het vertrouwen van de burgers blijft mijn prioriteit. Dat vereist zorgvuldigheid, transparantie en blijvende waakzaamheid.

**02.03** **Dieter Keuten** (VB): Dank u voor uw antwoord, mevrouw de minister.

Het gaat inderdaad over de bescherming van de privacy en het vertrouwen in de instellingen, maar het gaat ook over schade. We zijn daarom erg benieuwd naar de schadeclaims in Nederland. In ons land zijn nog niet veel cases van schadeclaims bekend, maar ik vrees dat die er wel zullen komen, als er aan het huidige tempo data worden gelekt. Persoonsgegevens worden op allerlei manieren gestolen en vervolgens wordt het door identiteitsdiefstal heel gemakkelijk om mensen op te lichten. Dat blijft dus een belangrijk aandachtspunt.

Ik heb ook goed genoteerd dat een lek binnen 72 uur bij de GBA gemeld moet worden. Dat komt in mijn volgende vraag ook terug. Ik vrees dat dat in veel gevallen niet binnen die korte termijn gebeurt.

Ten slotte kijk ik samen met u uit naar de voorgestelde aanpassingen van de privacywet, die van 2018 dateert, als ik mij niet vergis. De vorige directie van de GBA gaf in april al aan dat de privacywet een evaluatie en aanscherping verdient. Ik hoop dat u daar snel werk van maakt.

*Het incident is gesloten.  
L'incident est clos.*

**03** **Vraag van Dieter Keuten aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De datalekken bij Belfius, Orange en KBC" (56007779C)**

**03** **Question de Dieter Keuten à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Les fuites de données chez Belfius, Orange et KBC" (56007779C)**

**03.01** **Dieter Keuten** (VB): In ons land zijn er nog geen datalekken van medische gegevens op grote schaal, zoals in Nederland. Deze zomer hebben we echter wel over datalekken mogen vernemen bij Belfius, Orange en KBC. Het gaat ook niet om kleine organisaties, wel om organisaties die beschikken over zeer veel en soms ook gevoelige informatie. Een KBC-bedrijfsklant heeft niet alleen zijn eigen transactiegegevens ontvangen, maar ook die van andere klanten. Bij Orange was het een computerhacker die gegevens van maar liefst 850.000 klanten buitmaakte. Bij Belfius waren 4.000 klanten betrokken bij een incident. Het ging om 4.000 klanten die een verkeerde brief ontvingen, waarbij rekeninguittrekels van andere klanten zaten.

Mevrouw de minister, welke gevolgen zijn er reeds gegeven aan de recente datalekken? Hoe verklaart u het gebrek aan data-encryptie bij dergelijke grote organisaties? Kunt u toelichting geven bij de lopende onderzoeken van de Gegevensbeschermingsautoriteit? In het geval van Orange werd het lek pas na drie weken gecommuniceerd – of kwam het pas na drie weken in de media – wat ver verwijderd is van de 72 uur waar we het net over hadden.

Zijn er sancties als een melding te laat wordt gedaan bij de GBA? KBC deed er bovendien alles aan om het incident buiten de media te houden en ook de fout van Belfius kwam pas meer dan een maand na de feiten in de media. Wordt er ook opgetreden tegen die laattijdige communicatie of tegen pogingen om dergelijke datalekken uit de openbaarheid te houden? Worden er controles uitgevoerd om

soortgelijke incidenten te vermijden? Wordt er proactief gewerkt door de GBA of andere instanties om grote organisaties zoals Belfius, Orange en KBC te controleren? Zult u bijkomende maatregelen treffen en kunnen de slachtoffers op compensatie rekenen? Ik ben benieuwd.

**03.02** Minister **Vanessa Matz**: De recente datalekken bij Belfius, KBC en Orange tonen nogmaals aan hoe cruciaal gegevensbescherming is voor het vertrouwen van de burgers en voor de digitale veiligheid.

Volgens de AVG moeten organisaties persoonsgegevens goed beveiligen. Bij een datalek moet binnen de 72 uur melding worden gemaakt bij de Gegevensbeschermingsautoriteit en indien er een hoog risico is ook aan de betrokkenen.

De GBA kan sancties opleggen tot 20 miljoen euro of 4 % van de wereldwijde omzet. Orange heeft al extra maatregelen genomen om de impact te beperken. Zo verplicht het BIPT dat een consument zijn overstap naar een andere operator bevestigt om fraude via simswapping tegen te gaan.

Het CCB en het BIPT onderzoeken de oorzaken en de verantwoordelijkheden, en volgen op of de NIS2-regels correct toegepast zijn. De GBA bekijkt of de betrokken organisaties hun verplichtingen nagekomen zijn. Bij Orange zou het lek te wijten zijn aan organisatorische tekortkomingen, maar de controles lopen nog. De eindbeslissingen zullen worden gepubliceerd op de website van de GBA.

Datalekken moeten niet aan de pers gemeld worden, maar wel aan de GBA en aan de betrokkenen. Zowel de GBA als het BIPT voert controles uit en legt indien nodig maatregelen op. De slachtoffers kunnen gerechtelijke stappen voor schadevergoeding ondernemen.

Deze incidenten tonen het belang van strikte gegevensbescherming aan. De bevoegde autoriteiten zijn tussenbeide gekomen en ik heb de administratie gevraagd de privacywet te evalueren en indien nodig wijzigingen voor te bereiden in overleg met de sectoren.

**03.03** **Dieter Keuten** (VB): Mevrouw de minister, ik kijk uit naar de conclusies van de GBA, die vervolgens op haar website gepubliceerd zullen worden. U meldde dat het verplicht is om binnen de 72 uur aangifte te doen bij de GBA en om dit aan de betrokkenen te melden indien er een hoog risico is. 'Hoog risico' is natuurlijk een vaag begrip. Als er persoonsgegevens gestolen worden bij een bank, dan houdt dat altijd een hoog risico in.

Wij hebben vastgesteld dat als die betrokkenen vervolgens naar de pers willen stappen, zij onder druk worden gezet en er deurwaarders worden gestuurd om hen af te raden hun verhaal te doen. Dat is een praktijk die wij ook zouden moeten veroordelen.

Wat de gegevens betreft die bij Orange gestolen zijn, ben ik blij te horen dat Orange maatregelen heeft genomen, zodat er geen simswapping kan plaatsvinden, maar die klantgegevens zijn ondertussen wel gewoon te koop op het darkweb. Het is bijzonder onrustwekkend te horen dat het in het geval van Orange niet ging om menselijke fouten, maar om organisatorische tekortkomingen. Dat is een teken dat er daar iets serieus mis is.

Ten slotte, u zegt opnieuw dat de privacywet geëvalueerd moet worden. Wij blijven daarnaar uitkijken. Er zal echter ook proactief gewerkt moet worden om grote organisaties te controleren en te testen. Mensen, medewerkers, iedereen moet op een proactieve manier gesensibiliseerd worden om hier niet ten prooi aan te vallen.

*Het incident is gesloten.  
L'incident est clos.*

**04** **Vraag van Dieter Keuten aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De digitale beveiliging van ondernemingen" (56007780C)**

**04** **Question de Dieter Keuten à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "La sécurisation numérique des entreprises" (56007780C)**

**04.01** **Dieter Keuten** (VB): Mevrouw de minister, kleine ondernemingen vallen niet onder de NIS2-

richtlijn, die bedrijven verplicht hun cyberwaakzaamheid te verhogen, terwijl ook kleine bedrijven alsmaar vaker het slachtoffer worden van cyberaanvallen.

Volgens het Centrum voor Cybersecurity zou tweestapverificatie bijvoorbeeld een absolute minimummaatregel moeten zijn, maar veel kleine bedrijven maken daar onvoldoende gebruik van. Onderzoek van een cyberverzekeraar toont bovendien aan dat de grote meerderheid van de Belgische kmo's onvoldoende maatregelen neemt om hun digitale veiligheid te waarborgen.

Welke maatregelen zult u nemen om ook kleinere bedrijven bewust te maken van hun digitale kwetsbaarheid?

Op welke steun kunnen die ondernemingen en zelfstandigen daarvoor rekenen?

Hebt u daarover overleg gehad, bijvoorbeeld met uw collega bevoegd voor kmo en middenstand?

**04.02** Minister **Vanessa Matz**: Mijnheer Keuten, kleine bedrijven zijn erg kwetsbaar voor cyberaanvallen. Ze beschikken vaak niet over voldoende middelen om zich te beschermen, terwijl ze steeds vaker een doelwit zijn. Daarom is het belangrijk dat de overheid hen ondersteunt en bewustmaakt van de problematiek.

Het Centrum voor Cybersecurity België heeft verschillende tools ontwikkeld om hen te helpen. Het CyberFundamentals Framework biedt eenvoudige stappen om de beveiliging te verbeteren en het risico op een aanval te verkleinen. Het platform Safeonweb@work geeft gratis praktische diensten, waarschuwingen, rapporten over kwetsbaarheden, voorbeelden van veilig beleid en webinars in het Nederlands en het Frans. Het CCB voert ook jaarlijkse bewustmakingscampagnes onder andere over het belang van tweestapverificatie en publiceert praktische gidsen voor bedrijven.

Die initiatieven gebeuren samen met partners zoals UNIZO, UCM en de Cyber Security Coalition. Het Europees Comité voor gegevensbescherming, inclusief de GBA, geeft bijkomende adviezen en richtlijnen.

Voor meer informatie over cyberveiligheid verwijs ik naar mijn collega, de eerste minister. Zelf zorg ik ervoor dat de bescherming van persoonsgegevens centraal blijft en werk ik samen met het BIPT om de Data Act en de Data Governance Act correct toe te passen.

**04.03** **Dieter Keuten** (VB): Bedankt voor uw antwoord, mevrouw de minister.

Bewustmakingscampagnes zijn zeker waardevolle initiatieven om burgers en ondernemingen, in het bijzonder kleine ondernemingen, te informeren. We moeten echter meer doen om het publiek wakker te schudden. Het is niet de vraag of een onderneming gehackt zal worden, maar wanneer dat zal gebeuren. Dat blijkt duidelijk uit de cijfers.

Bedrijven zijn kwetsbaar voor afpersing. Nog bij het begin van afgelopen week moesten we vaststellen hoe een toeleverancier van de luchthaven van Zaventem werd afgeperst om systemen vrij te geven of de diefstal van persoonsgegevens te voorkomen. Over dergelijke gevallen wordt veel te weinig gecommuniceerd. Als er wel informatie beschikbaar zou zijn over de bedragen die in dergelijke gevallen betaald moeten worden, dan zou dat sensibiliserend werken. Het zou andere ondernemingen kunnen doen inzien welke enorme risico's ze lopen bij een aanval door hackers. Daarom denk ik dat er, naast bewustmakingscampagnes, ook veel meer over de hacks en de daaruit voortvloeiende schade moet worden gecommuniceerd. Dan zullen veel meer bedrijven en personen zich bewust worden van het gevaar.

Ik hoop dat u de nodige stappen zult zetten om hacking uit de taboesfeer te halen en te communiceren over de gevolgen ervan.

*L'incident est clos.*

*Het incident is gesloten.*

**05** Question de Patrick Prévot à Vanessa Matz (Action et Modernisation publiques, Entreprises publiques, Fonction publique, Gestion immobilière de l'État, Numérique et Politique scientifique) sur "Le règlement européen CSAM (Child Sexual Abuse Material)" (56008207C)

**05** Vraag van Patrick Prévot aan Vanessa Matz (Modernisering van de overheid, Overheidsbedrijven, Ambtenarenzaken, Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid) over "De CSAM-verordening (Child Sexual Abuse Material)" (56008207C)

**05.01** **Patrick Prévot** (PS): Madame la ministre, comme c'est une matière quelque peu technique, et afin de faire gagner du temps à tout le monde, je m'en réfère à ma question telle que déposée par écrit.

*Madame la ministre, la proposition de règlement européen CSAM qui vise à lutter contre la diffusion de contenus pédopornographiques suscite beaucoup de questionnements.*

*Pour être synthétique, le CSAM mettrait en place un système qui obligerait les plateformes à scanner les contenus échangés en amont de leur diffusion en ligne – que ces plateformes soient cryptées ou non. À l'heure actuelle, la réglementation est axée sur le retrait de contenus une fois identifiés. Le CSAM cherche à renverser la balance en s'attaquant directement à la source de la personne qui serait sur le point de partager une image à caractère pédopornographique.*

*Par quelle technique? Celle du "client-side scanning", une technique qui consiste à analyser le contenu d'un message sur l'appareil de l'utilisateur avant qu'il ne soit envoyé. Dans un article du 20 septembre dernier publié sur le site de la RTBF, j'apprends que le texte est actuellement discuté au sein des États membres de l'UE et prévoit un garde-fou qui permettrait de rallier les actuels opposants au texte. Ce garde-fou, c'est la mise en place d'un centre d'expertise européen qui servirait de cadre à l'application de la législation.*

*Madame la ministre, j'en viens à mes questions qui sont multiples.*

*Tout d'abord, quelle est la position de la Belgique sur la dernière version du CSAM? A-t-elle fait l'objet d'un consensus au sein des entités fédérées? Quelles évaluations la Belgique a-t-elle remise le 12 septembre dernier, date-butoir de l'analyse de cette dernière version?*

*Ensuite, je lis que les plateformes devraient vérifier si des photos ou vidéos issues de bases de données contenant des contenus pédopornographiques déjà identifiés circulent sur leurs réseaux et, le cas échéant, d'en bloquer la diffusion: quelles sont ces bases de données? Depuis quand existent-elles? Qui les alimente et les contrôle?*

*Troisièmement, ce "EU Centre" qui serait un garde-fou fonctionnerait comme centre de tri et donc comme intermédiaire: a-t-on une idée de l'enveloppe budgétaire que ce centre réclamerait ainsi que ses ressources humaines? Où se situerait-il?*

*Enfin, quel rôle jouerait l'IBPT en cas de mise en vigueur de ce CSAM à l'heure où l'institution est déjà surchargée de travail (IA Act, DSA, etc.)?*

**05.02** **Vanessa Matz**, ministre: Monsieur Prévot, je vous remercie pour votre sollicitude.

Elle est bien utile après quatre commissions de questions orales. Néanmoins, le sujet est d'importance et s'il est technique, il est hautement important de pouvoir répondre au mieux à cette question parce que ce règlement soulève bien des inquiétudes.

La pédopornographie est un fléau qui touche des victimes toujours plus jeunes et dont les images circulent massivement sur les plateformes et réseaux sociaux. L'accord de gouvernement fait de la lutte contre l'exploitation et la diffusion de ces contenus une priorité absolue. Le règlement CSAM, en discussion au niveau européen, constitue une étape importante. La Belgique adopte une approche constructive même si sa position définitive n'est pas encore arrêtée.

Le compromis proposé par la présidence danoise s'inspire très largement de la proposition belge de 2024. Le texte prévoit que ce sont d'abord les fournisseurs de services qui doivent mettre en place des mesures pour réduire la diffusion de contenus pédopornographiques. Ce n'est qu'en cas de risque élevé persistant qu'une détection ciblée – j'insiste – temporaire pourra être décidée par une autorité

judiciaire ou indépendante.

Le centre européen qui serait créé générerait une base de données commune à l'Union. Celle-ci ne contient pas les images en elles-mêmes, mais des empreintes numériques issues exclusivement d'autorités judiciaires ou reconnues, comme Interpol ou l'Internet Watch Foundation. Ce mécanisme existe déjà depuis plusieurs années et garantit la fiabilité des ajouts.

Les discussions se poursuivent encore, notamment sur le budget et sur la désignation des autorités nationales qui seraient compétentes. Je dois dire que mon cabinet est en troisième ligne sur ce dossier, puisque ce sont les ministres de l'Intérieur, de la Justice et du Numérique qui sont impliqués.

Je regrette que circulent parfois des informations incomplètes sur ce dossier technique, mais cela montre aussi l'importance de l'enjeu pour la société civile. Pour ma part, je suis ce projet avec la plus grande vigilance afin de maintenir l'équilibre entre la protection des mineurs et le respect des libertés fondamentales.

**05.03 Patrick Prévot (PS):** Madame la ministre, je vous remercie pour cette réponse à une question importante.

J'entends que la position définitive de la Belgique n'est pas encore pleinement arrêtée. Même si vous intervenez en troisième ligne en tant que ministre chargée du Numérique, comme vous l'avez rappelé, après les ministres de l'Intérieur et de la Justice, il me semblait intéressant d'obtenir votre éclairage. Une question identique sera donc également posée à vos deux collègues.

J'entends, par ailleurs, ce petit regret que certaines informations qui circulent soient erronées et je le souligne. Tout comme vous, j'estime qu'il faut trouver une solution qui maintienne l'équilibre entre la protection des enfants et la liberté individuelle, qui nous est chère. Merci d'avoir fait le point sur ce dossier.

*L'incident est clos.*

*Het incident is gesloten.*

Le **président**: Voilà qui nous amène à la fin des questions orales adressées à Mme la ministre Matz, que je remercie pour sa présence.

Chers collègues, merci pour vos questions. Je remercie également les services.

*De behandeling van de vragen eindigt om 13.59 uur.*

*Le développement des questions se termine à 13 h 59.*