CDDH-IA(2025)2
31/01/2025

STEERING COMMITTEE FOR HUMAN RIGHTS

COMITÉ DIRECTEUR POUR LES DROITS HUMAINS

(CDDH)

DRAFTING GROUP ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

GROUPE DE RÉDACTION SUR LES DROITS HUMAINS ET L'INTELLIGENCE ARTIFICIELLE

(CDDH-IA)

Compilation of replies to the questionnaire to member States on human rights and artificial intelligence (CDDH-IA(2024)10REV)[1]

Compilation des réponses au questionnaire aux États membres sur les droits humains et l'intelligence artificielle (CDDH-IA(2024)10R)[2]

[1] Andorra, Cyprus, Czechia, Denmark, France, Georgia, Greece, Italy, Latvia, Liechtenstein, Lithuania, Malta, Monaco, Montenegro, Netherlands, Poland, San Marino, Serbia, Slovakia, Spain, Switzerland, Türkiye, United Kingdom, Ukraine

[2] Andorre, Chypre, Danemark, France, Géorgie, Grèce, Italie, Lettonie, Liechtenstein, Lituanie, Malte, Monaco, Monténégro, Pays-Bas, Pologne, Saint-Marin, Serbie, Slovaquie, Espagne, Suisse, Türkiye, Royaume-Uni, Ukraine.

Table of Contents

QUESTION 1

ENGLISH

Have your country's domestic courts addressed any cases involving artificial intelligence and human rights?

If so, please provide relevant cases, including the following information:

(i) A brief summary of the facts, including details of the AI technology involved (e.g., predictive policing, facial recognition, automated decision-making) and the area of activity in which it was applied.
(ii) The specific human rights at issue, if identified.
(iii) A summary of the domestic court's reasoning and decision.
(iv) Any reference made by the domestic court to the ECHR, ESC or other international human rights standards.

FRENCH

Les tribunaux nationaux de votre pays ont-ils examiné des affaires impliquant l'intelligence artificielle et les droits humains ?

Dans l'affirmative, merci de fournir des détails pertinents sur l'affaire, y compris les informations suivantes :

(i) Un résumé des faits, y compris des détails sur la technologie d'IA impliquée (par exemple, la police prédictive, la reconnaissance faciale, la prise de décision automatisée) et le domaine d'activité dans lequel elle a été appliquée.
(ii) Les droits humains spécifiques en cause, s'ils sont identifiés
(iii) Un résumé du raisonnement et de la décision de la juridiction nationale
(iv) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains

ANDORRA / *ANDORRE*

Les tribunaux de la Principauté d'Andorre n'ont, à ce jour, pas examiné d'affaires impliquant l'intelligence artificielle et les droits humains.
Bien qu'il n'y ait pas d'exemples spécifiques de cas judiciaires, le contexte actuel – notamment le Code éthique sur l'IA (approuvé le 2 mai 2024) – fournit un cadre de base pour faciliter le développement et l'utilisation de l'IA en harmonie avec tout ce qui concerne les droits de l'homme. Cela constitue un élément clé pour éviter les conflits juridiques à l'avenir et garantir que l'utilisation de l'IA soit responsable et bénéfique pour la société.

CYPRUS / *CHYPRE*

According to information received from the Supreme Court's Registry in Cyprus, domestic courts have not addressed any cases involving artificial intelligence and human rights.

CZECHIA / *TCHÉQUIE*

The Government are not aware of any judicial cases regarding artificial intelligence (AI) and human rights *stricto sensu* in the Czech Republic. However, there was a dispute between two private persons that involved protection of property (Article 1 of Protocol No. 1 to the Convention).

In 2023 the Municipal Court in Prague delivered judgment no 10 C 13/2023-16 regarding the use of AI system (DALL-E) and protection of intellectual property. The plaintiff sought recognition of his authorship to the image generated by the AI system. The court addressed the following question: Is it possible to consider images created by artificial intelligence based on human input as a work of authorship? The court assessed whether the person's input – a so-called "prompt" to the AI system – was sufficient to confer authorship. At first, the court concluded that the image created by the AI system did not meet statutory definition of a "work of authorship". That is because the AI system as such cannot be considered "an individual" capable of the creative act of individual creation according to the relevant provision. At the same time, the plaintiff did not produce sufficient evidence to show that the image was truly created based on his specific prompt. According to the court, conditions of authorship under the Czech Copyright Act cannot be met without concrete evidence supporting the individual's claim of significant human involvement in the creative process. However, the court did not completely rule out that AI-generated works could be granted copyright protection in the future if a sufficient level of human creative input is demonstrated.

DENMARK / *DANEMARK*

No reply.

FRANCE

1. <u>Décisions comportant une référence directe à l'intelligence artificielle</u>

a) En général

- CE, 30 décembre 2021, *Société Gerbi Avocat Victimes et Préjudices et autres*, n^{os} 440376, 440976, 442327, 442361, 442935

(i) Un résumé des faits :

La Société Gerbi Avocat Victimes et Préjudices et d'autres requérants demandent l'annulation pour excès de pouvoir du décret n° 2020-356 du 27 mars 2020 portant création d'un traitement automatisé de données à caractère personne dénommé « Datajust ».

(ii) La technologie d'IA mise en cause ;

Création d'un traitement automatisé de données à caractère personnel ayant pour but le développement d'un outil d'aide à la décision des juges, fondé sur une intelligence artificielle.

Datajust, projet qui n'a à ce stade pas abouti, devait recenser, par type de préjudice, les montants demandés et offerts par les parties à un litige ainsi que les montants alloués aux victimes en indemnisation de leur préjudice corporel. Cela devait permettre de tendre vers une harmonisation des montants d'indemnisation de préjudices comparables.

(iii) Les droits humains en question ;

Droit au respect de la vie privée, protection des données à caractère personnel.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Le décret attaqué se borne à autoriser la collecte de données nécessaires au développement d'un algorithme en matière d'indemnisation du préjudice corporel sans déroger à la loi du 6 janvier 1978. Il n'a ni pour objet, ni pour effet de fixer des règles relatives aux garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Le traitement autorisé par le décret attaqué a pour objet la mise au point d'un algorithme destiné à l'élaboration d'un référentiel indicatif d'indemnisation des préjudices corporels ayant vocation à être utilisé pour évaluer ces préjudices dans le cadre du règlement tant amiable que juridictionnel des litiges. Il tend ainsi à assurer un accès plus facile à la jurisprudence sur l'indemnisation des préjudices corporels afin de garantir l'accessibilité et la prévisibilité du droit. Au surplus et à ce stade, ce traitement, dont la durée est réduite à deux ans, est limité à la phase de développement d'un outil d'intelligence artificielle, n'a qu'un caractère expérimental et n'a pas vocation, à ce stade, à être mis à la disposition des magistrats ou des parties. Par ailleurs, aux termes de l'article 2 du décret attaqué, les noms et prénoms des personnes physiques parties aux instances ayant fait l'objet des décisions de justice rendues en appel entre le 1er janvier 2017 et le 31 décembre 2019 à partir desquelles les données nécessaires à la mise au point de l'algorithme sont extraites, doivent être occultés préalablement à leur transmission au secrétariat général du ministère de la justice. Eu égard au grand nombre des décisions juridictionnelles à traiter, il ne peut pas être soutenu que l'information individuelle de chaque personne concernée n'exigerait pas d'efforts disproportionnés. Ainsi, le moyen tiré de ce que l'exclusion du droit à l'information serait excessive ou méconnaitrait l'article 8 de la Charte des droits fondamentaux de l'Union européenne doit être écarté. Si les dispositions citées au point précédent mettent à la charge du responsable du traitement l'obligation de rendre l'information publiquement disponible, elles n'imposent pas que l'acte portant création du traitement rappelle cette obligation ni qu'il détermine les modalités de sa mise en œuvre.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Article 8 de la Convention EDH
- Article 8 de la Charte des droits fondamentaux de l'Union européenne

b) Technologies de reconnaissance faciale

- CE, avis sur un projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, 15 décembre 2022, n° 406383

(i) Un résumé des faits :

Le Conseil d'Etat a été saisi le 22 novembre 2022 d'un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024. Ce projet de loi a été modifié par trois saisines rectificatives reçues les 29 novembre, 2 et 8 décembre 2022 en ce qui concerne le texte du projet et, s'agissant de l'étude d'impact, les 25 novembre 2022, 7 et 12 décembre 2022. Le projet de loi comprend plusieurs mesures, concernant divers domaines, nécessaires à l'organisation des jeux

et notamment des dispositions relatives à l'utilisation de traitements algorithmiques sur des images afin de détecter et signaler en temps réel des événements prédéterminés susceptibles de menacer la sécurité des personnes.

(ii) La technologie d'IA mise en cause ;

Systèmes d'intelligence artificielle appliqués aux images de vidéoprotection.

(iii) Les droits humains en question ;

Droit au respect de la vie privée, liberté d'aller et venir, libertés d'opinion et de manifestation.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Le recours à des analyses automatisées est réservé, à titre expérimental et jusqu'au 31 décembre 2024, à des manifestations qui par leur ampleur ou leurs circonstances sont particulièrement exposées à des risques graves d'atteinte à la sécurité des personnes notamment du fait d'actes de terrorisme. Les traitements ne collectent ni n'utilisent aucune donnée biométrique et ne peuvent, en particulier, recourir à la reconnaissance faciale. Il leur est interdit de procéder à aucun rapprochement, interconnexion ou mise en relation automatisée avec d'autres traitements de données personnelles. Ils procèdent exclusivement à un signalement d'attention et ne peuvent produire aucun autre résultat, ni fonder par eux-mêmes aucune décision individuelle ou acte de poursuite. La finalité et la fonctionnalité des systèmes sont ainsi très strictement bornées. Le Conseil d'Etat propose d'ajouter à ces garanties le principe de primauté humaine, assurant qu'à tout instant le traitement ne fonctionne que sous la supervision des personnes qui le mettent en œuvre. Le Conseil d'Etat estime que cette expérimentation, limitée dans le temps et dans l'espace, telle qu'elle est régie et encadrée par le projet de loi ainsi précisé, ne se heurte à aucune objection d'ordre constitutionnel ou conventionnel et est susceptible d'assurer une plus grande efficacité du maintien de l'ordre et de la sécurité des manifestations d'ampleur inédites qui vont se dérouler, notamment pendant la période des jeux Olympiques et Paralympiques. L'intervention de la CNIL comme autorité de contrôle, aussi bien au stade de l'autorisation du déploiement du traitement que durant sa mise en œuvre et son évaluation, assure une supervision constante de l'expérimentation de nature à prévenir les risques susceptibles d'être rencontrés.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Mention de l'absence d'objection d'ordre conventionnel à cette expérimentation

➢ Décision du Conseil constitutionnel n° 2021-834 DC du 20 janvier 2022

(vi) Un résumé des faits :

Saisi de quatre articles de la loi relative à la responsabilité pénale et à la sécurité intérieure, le Conseil constitutionnel censure partiellement les dispositions relatives au recours aux drones dans le cadre de la police administrative et assortit de cinq réserves d'interprétation le reste des dispositions contestées.

(vii) La technologie d'IA mise en cause ;

Traitements d'images issues de caméras installées sur des aéronefs, y compris sans personne à bord, dans le cadre d'opérations de police administrative.

(viii) Les droits humains en question ;

Droit au respect de la vie privée.

(ix) Un résumé du raisonnement et de la décision de la Cour ;

Les services de police nationale et de gendarmerie nationale ainsi que les militaires déployés sur le territoire national ne peuvent être autorisés à faire usage de ces dispositifs qu'aux fins d'assurer la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques de commission de certaines infractions, la protection des bâtiments et installations publics et de leurs abords immédiats particulièrement exposés à des risques d'intrusion ou de dégradation, la sécurité des rassemblements de personnes sur la voie publique ou dans des lieux ouverts au public lorsque ces rassemblements sont susceptibles d'entraîner des troubles graves à l'ordre public, la prévention d'actes de terrorisme, la régulation des flux de transport aux seules fins du maintien de l'ordre et de la sécurité publics, la surveillance des frontières et le secours aux personnes. Par une première réserve d'interprétation, le Conseil constitutionnel juge que l'autorisation du préfet déterminant cette finalité et le périmètre strictement nécessaire pour l'atteindre ainsi que le nombre maximal de caméras pouvant être utilisées simultanément dans le même périmètre géographique ne saurait, sans méconnaître le droit au respect de la vie privée, être accordée qu'après que le préfet s'est assuré que le service ne peut employer d'autres moyens moins intrusifs au regard de ce droit ou que l'utilisation de ces autres moyens serait susceptible d'entraîner des menaces graves pour l'intégrité physique des agents. Par une deuxième réserve d'interprétation, le Conseil constitutionnel juge que le renouvellement d'une telle autorisation ne saurait, sans méconnaître le droit au respect de la vie privée, être décidé par le préfet sans qu'il soit établi que le recours à ces dispositifs aéroportés demeure le seul moyen d'atteindre la finalité poursuivie. Par une troisième réserve d'interprétation, le Conseil constitutionnel juge que ces dispositions ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés.

(x) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

Pas de référence dans cette décision

- CE, 26 avril 2022, *Association la quadrature du net*, n° 442364

(xi) Un résumé des faits :

L'Association la quadrature du net demande l'annulation pour excès de pouvoir du refus d'abrogation des dispositions autorisant l'enregistrement dans le TAJ d'une « photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale » concernant respectivement les personnes physiques mises en cause et les personnes physiques faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition.

(xii) La technologie d'IA mise en cause ;

Dispositif de reconnaissance faciale.

(xiii) Les droits humains en question ;

Droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et la liberté d'expression et d'information.

(xiv) Un résumé du raisonnement et de la décision de la Cour ;

La mise en œuvre du TAJ fait l'objet d'un suivi par un magistrat désigné à cet effet par le ministre de la justice en application des articles 230-9 et R. 40-32 du même code et est soumise au

contrôle de la Commission nationale de l'informatique et des libertés, laquelle peut s'assurer du respect des droits des personnes concernées mentionnés à l'article R. 40-33. Il appartient enfin au responsable de traitement, conformément à l'article 32 de la loi du 6 janvier 1978, de prendre les mesures de sécurité appropriées au regard de la sensibilité des données en cause. Il suit de là que le traitement litigieux comporte des garanties appropriées pour les droits et libertés des personnes concernées et n'institue pas, contrairement à ce qui est soutenu, un « dispositif disproportionné ». Les articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne garantissent le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et la liberté d'expression et d'information. Il ressort de la jurisprudence de la Cour de justice de l'Union européenne, notamment de sa décision La Quadrature du Net et autres du 6 octobre 2020 (C-511/18, C-512/18 et C-520/18), d'une part, que l'article 52, paragraphe 1, de la même Charte admet des limitations à l'exercice de ces droits et libertés, pour autant que celles-ci soient prévues par la loi, qu'elles respectent le contenu essentiel de ces droits et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui, d'autre part, que la protection du droit fondamental au respect de la vie privée exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire et, enfin, qu'au nombre des objectifs d'intérêt général reconnus par le droit de l'Union figurent la lutte contre la criminalité et la sauvegarde de la sécurité publique.

(xv) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne

- Traitements d'images au moyen de dispositifs de captation installés sur des aéronefs :

  - CE, 30 décembre 2024, Ligue des droits de l'homme, n°s 473506,473546,473749,473867, T.

(i) Un résumé des faits :

La Ligue des droits de l'homme et d'autres requérants demandent l'annulation pour excès de pouvoir du décret n° 2023-283 du 19 avril 2023 relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs pour des missions de police administrative.

(ii) La technologie d'IA mise en cause ;

Traitements d'images au moyen de dispositifs de captation installés sur des aéronefs.

(iii) Les droits humains en question ;

Droit au respect de la vie privée et droit à la protection des données à caractère personnel.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Le recours à des dispositifs aéroportés ne peut être autorisé par le préfet en application des dispositions du IV de l'article L. 242-4 du code de la sécurité intérieure que s'il est proportionné au regard de la finalité poursuivie, et sous les réserves formulées par le Conseil constitutionnel dans sa décision n° 2021-834 DC du 20 janvier 2022. L'autorisation ne saurait davantage être renouvelée sans qu'il ne soit établi que le recours à des dispositifs aéroportés demeure le seul moyen d'atteindre la finalité poursuive. L'acte d'autorisation, notamment ses modalités de publication, sont susceptibles de faire l'objet d'un recours pour excès de pouvoir devant le juge

administratif pouvant être assorti, le cas échéant, d'une demande de suspension de l'exécution de l'acte en cas d'urgence. Il appartient alors à l'autorité administrative de procéder, dans toute la mesure du possible, à la publication de l'acte d'autorisation dans un délai permettant de saisir utilement le juge administratif. Le traitement de données à caractère personnel issu des captations et enregistrements réalisés par les dispositifs aéroportés ne peut pas procéder à la captation du son. Il ne peut ni comporter de traitements automatisés de reconnaissance faciale, ni procéder à des rapprochements, interconnexions ou mises en relation automatisées avec d'autres traitements. Si des données personnelles à caractère sensible sont susceptibles d'être enregistrées dans le traitement, elles ne peuvent l'être que dans la mesure où elles sont strictement nécessaires à la poursuite des finalités du traitement. Ces données sensibles excluent toute sélection d'une catégorie particulière des personnes à partir de ces seules données. Leur durée de conservation est limitée à sept jours à compter de la fin du déploiement du dispositif. Dans ces conditions, et alors que le périmètre des données susceptibles d'être collectées n'est pas, par ailleurs, excessif au regard des finalités du traitement, l'autorisation d'enregistrement de données personnelles à caractère sensible prévue par le décret attaqué présente des garanties appropriées au sens de l'article 88 de la loi du 6 janvier 1978 et de la directive 2016/680 du 27 avril 2016. Elle ne méconnaît pas, par elle-même, les exigences posées par les articles 4 et 6 de cette loi.

(v) **Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.**

- Article 16 de la convention internationale des droits de l'enfant.

➢ CE, juge des référés, 21 décembre 2023, Communauté de communes Cœur Côté Fleurie, n° 489990

(i) Un résumé des faits :

La Ligue des droits de l'homme, le Syndicat de la magistrature et l'Union syndicale Solidaires, d'une part, l'Association de défense des libertés constitutionnelles et le Syndicat des avocats de France, d'autre part, ont demandé au juge des référés du tribunal administratif de Caen, statuant sur le fondement de l'article L. 521-2 du code de justice administrative, d'enjoindre à la communauté de communes Cœur Côte Fleurie de cesser immédiatement l'usage du logiciel édité par la société BriefCam. Par une ordonnance du 22 novembre 2023, ce juge des référés a enjoint à la communauté de communes Cœur Côte Fleurie de procéder, dans un délai de cinq jours, à l'effacement des données à caractère personnel contenues dans le fichier initialement constitué et dans toutes les copies, totales ou partielles, qui auraient pu en être faites, à l'exception d'un seul exemplaire à placer sous séquestre auprès de la Commission nationale de l'informatique et des libertés (CNIL) dans un délai d'un mois. La communauté de communes Cœur Côte Fleurie relève appel de cette ordonnance.

(ii) La technologie d'IA mise en cause ;

Technologie de reconnaissance faciale et de télésurveillance algorithmique en temps réel.

(iii) Les droits humains en question ;

Droit au respect de la vie privée et liberté d'aller et venir.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

S'il n'est pas contesté que le logiciel litigieux dispose de fonctionnalités qui permettent de procéder à de la reconnaissance faciale, alors que l'usage de telles techniques est légalement interdit, il résulte des déclarations en appel de la communauté de communes Cœur Côte Fleurie,

qui n'avait pas défendu en première instance, que ces fonctionnalités, pourtant présentes depuis 2018 à la suite d'une mise à jour du logiciel, n'ont jamais été activées dans son ressort. S'il est vrai que le logiciel en cause comporte, dans le module « Review », des fonctionnalité d'analyse des images, notamment par l'application de filtres, par exemple par sexe, taille ou par type de vêtements, ou d'analyse des comportements de déplacement, la communauté de communes indique, que le logiciel n'est pas utilisé pour assurer, par la mise en œuvre de traitements algorithmiques, un suivi de manière automatisée des personnes ou détecter des événements et déclencher des alertes en temps réel, le module « Respond » dont peut être équipé le logiciel n'étant d'ailleurs pas disponible. Déployé dans l'intercommunalité depuis plusieurs années, pour un nombre limité de caméras, il apparaît, en l'état de l'instruction, que ce système, tel qu'il est calibré et peut raisonnablement être mobilisé, n'est utilisé que pour une relecture en différé, sur une zone et un temps limités, des images collectées par les caméras concernées, notamment en vue d'une analyse de véhicules et une recherche de plaques d'immatriculation, pour les besoins d'une enquête et participe au bon déroulement de celle-ci en réduisant les délais de lecture et d'exploitation de ces images. Enfin et en tout état de cause, il ressort d'une expertise technique menée à la demande de la communauté de communes que les opérations mises en œuvre pour assurer l'exécution de l'ordonnance attaquée ont causé la détérioration du logiciel, qui n'est plus fonctionnel, notamment en ce qu'il n'est plus possible d'importer des éléments vidéo et de les exploiter. Il en ressort également que les efforts pour le remettre en service, malgré le support de l'éditeur du logiciel, n'ont pas pu aboutir. Il en résulte qu'à la date de la présente ordonnance, aucune utilisation du logiciel n'est techniquement possible.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

Article 8 de la Convention EDH

- TA de Marseille, 27 février 2020, *La Quadrature du Net et autres*, n° 1901249

(i) Un résumé des faits :

Par la délibération n° 13-893 du 14 décembre 2018, le conseil régional de la région Provence-Alpes-Côte d'Azur (PACA) a, d'une part, lancé l'expérimentation du dispositif de contrôle d'accès virtuel dans les lycées « Ampère » (Marseille) et « Les Eucalyptus » (Nice) et, d'autre part, approuvé la convention tripartite d'expérimentation conclue avec la société Cisco International Limited et chacun des deux lycées et autorisé son président à les signer. Par la présente requête, l'association « La Quadrature du Net », la Ligue des droits de l'Homme, la fédération des conseils des parents d'élèves des écoles publiques des Alpes-Maritimes et le syndicat CGT Educ'Action des Alpes-Maritimes demandent au Tribunal l'annulation pour excès de pouvoir de cette délibération.

(ii) La technologie d'IA mise en cause ;

Dispositif de contrôle d'accès virtuel.

(iii) Les droits humains en question ;

Droit au respect de la vie privée, protection des données à caractère personnel.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Selon les termes de la délibération en cause, ce dispositif a pour finalités *« (…) d'apporter une assistance aux agents en charge du contrôle d'accès au lycée et de l'accueil afin de faciliter et réduire la durée des contrôles (pour les usagers réguliers du site comme pour les visiteurs occasionnels), lutter contre l'usurpation d'identité et détecter un déplacement non souhaité »*.

Cependant, la région PACA n'établit ni ne fait valoir que les finalités poursuivies s'attachant à la fluidification et la sécurisation des contrôles à l'entrée des lycées concernés constituent un motif d'intérêt public ni même que ces finalités ne pourraient être atteintes de manière suffisamment efficace par des contrôles par badge, assortis, le cas échéant, de l'usage de la vidéosurveillance. Les requérantes sont donc fondées à soutenir que le traitement de données biométriques institué par la région PACA ne satisfait pas aux exigences prévues par le a) de l'article 9 du règlement général sur la protection des données telles qu'éclairées notamment par ses articles 4 et 7, ni davantage aux conditions énoncées par le g) du même règlement, et qu'il n'entre dans aucune des exceptions énumérées par le 2 de l'article 9 du règlement général sur la protection des données. Elles sont, par suite, fondées à soutenir que la délibération qu'elles contestent est entachée d'illégalité au regard de l'article 9 du règlement général sur la protection des données.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Article 8 de la Convention EDH

2. <u>Décisions relatives à des traitements automatisés de données à caractère personnel, sans recours à de l'intelligence artificielle stricto sensu</u>

➢ CE, 26 octobre 2011, *Association pour la promotion de l'image et autres*, n° 317827, 317952,318013,318051,

(i) Un résumé des faits :

L'Association pour la promotion de l'image et plusieurs autres requérants demandent d'annulation pour excès de pouvoir du décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, ainsi que la circulaire n° INT/1/08/00105/C du 7 mai 2008 relative au choix des deux mille communes appelées à recevoir des stations d'enregistrement des données personnelles pour le nouveau passeport.

(ii) La technologie d'IA mise en cause ;

Un système de traitement automatisé centralisé des données à caractère personnel contenant l'image numérisée du visage et les empreintes digitales mais sans dispositif de reconnaissance faciale à partir de l'image numérisée du visage ni dispositif de recherche permettant l'identification à partir de l'image numérisée des empreintes digitales enregistrées dans ce traitement.

(iii) Les droits humains en question ;

Le droit à la vie privée et la liberté d'aller et venir

(iv) Un résumé du raisonnement et de la décision de la Cour ;

La finalité de la consultation des empreintes digitales contenues dans le traitement automatisé (qui est de confirmer que la personne présentant une demande de renouvellement d'un passeport est bien celle à laquelle le passeport a été initialement délivré ou de s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport) peut être atteinte de manière suffisamment efficace en comparant les empreintes figurant dans le composant électronique du passeport avec celles conservées dans le traitement, sans qu'il soit nécessaire que ce dernier en contienne davantage. Dès lors, inconventionnalité de la collecte et de la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique, qui ne sont ni adaptées, ni nécessaires, ni proportionnées à la finalité

du traitement. Le caractère centralisé du traitement a pour but de faciliter les démarches des usagers, de renforcer l'efficacité de la lutte contre la fraude documentaire et de garantir une meilleure protection des données recueillies. Ces finalités sont au nombre de celles qui justifient qu'il puisse être porté, par la création d'un traitement centralisé de données à caractère personnel, atteinte au droit des individus au respect de leur vie privée. Dès lors, conventionnalité du traitement centralisé en cause qui, compte tenu des restrictions et précautions dont il est assorti, est en adéquation avec ses finalités légitimes.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales
- Article 2-3 de son quatrième protocole additionnel
- Article 16 de la convention relative aux droits de l'enfant signée à New York le 26 janvier 1990

➢ CE, 11 mars 2013, *Association sos racisme, touche pas à mon pote*, n° 348613

(i) Un résumé des faits :

L'Association sos racisme, touche pas à mon pote demande l'annulation pour excès de pouvoir du décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et à la prévention des atteintes à la sécurité publique (GIPASP).

(ii) La technologie d'IA mise en cause ;

Un système de traitement de données à caractère personnel nécessaires à la poursuite de la finalité de préservation de la sécurité publique. Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie.

(vi) Les droits humains en question ;

L'égalité de devant la loi, la présomption d'innocence, le respect de la vie privée.

(vii) Un résumé du raisonnement et de la décision de la Cour ;

Le traitement GIPASP autorise la collecte de collecte de données dont la finalité est de prévenir les risques d'atteinte à la sécurité publique. Dans ce cadre, la collecte des informations peut concerner notamment les personnes susceptibles d'être impliqués dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives. Les finalités de protection de l'ordre public et de prévention des risques de d'atteinte à la sécurité publique ainsi assignées au traitement sont légitimes et assorties des précisons suffisantes exigées par l'article 6 de la loi du 6 janvier 1978. Au regard de ces finalités, les données dont la collecte est autorisée sont pertinentes, adéquates et ne présentent pas un caractère excessif.

(viii) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Convention EDH)
- Article 16 de la convention relative aux droits de l'enfant signée à New York le 26 janvier 1990

- CE, 5 février 2020, *Unicef France et autres*, n° 428478, T.

(i) Un résumé des faits :

Le comité français pour le Fonds des Nations Unies pour l'enfance « UNICEF France » et plusieurs autres requérants demandent l'annulation pour excès de pouvoir du décret n° 2019-57 du 30 janvier 2019 relatif aux modalités d'évaluation des personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille et autorisant la création d'un traitement de données à caractère personnel relatif à ces personnes.

(ii) La technologie d'IA mise en cause ;

Traitement automatisé de données à caractère personnel

(iii) Les droits humains en question ;

Protection de l'intérêt supérieur de l'enfant et le droit au respect de la vie privée.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Le décret litigieux définit, en application de l'article L. 611-6-1 du code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA), les caractéristiques du traitement automatisé dans lequel peuvent être enregistrées certaines données à caractère personnel des personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille. Le but est d'aider à la détermination de l'identité de ces personnes en modifiant les dispositions applicables au traitement "application de gestion des dossiers des ressortissants étrangers en France" (AGDREF2) et au traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa ou "VISABIO". En revanche, le décret ne modifie pas l'étendue des obligations du président du conseil départemental en ce qui concerne l'accueil provisoire d'urgence des personnes se déclarant mineures et privées de la protection de leur famille, non plus que sa compétence pour évaluer, sur la base d'un faisceau d'indices, leur situation, notamment quant à leur âge, et ne l'autorise pas à prendre une décision qui serait fondée sur le seul refus de l'intéressé de fournir les informations nécessaires à l'interrogation ou au renseignement des traitements mentionnés ci-dessus ni sur le seul constat qu'il serait déjà enregistré dans l'un d'eux

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Articles 3 et 20 de la convention relative aux droits de l'enfant
- Articles 3 et 8 de la Convention EDH

- CE, 24 décembre 2021, *Ligue des droits de l'homme et autre*, n°s 447513,447973,448059,449299,449461, T.

(i) Un résumé des faits :

La Ligue des droits de l'homme et d'autres requérants demandent l'annulation pour excès de pouvoir du décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » (EASP).

(ii) La technologie d'IA mise en cause ;

Traitement automatisé de données à caractère personnel

(iii) Les droits humains en question ;

Droit au respect de la vie privée, droit à la liberté de pensée, de conscience et de religion, libertés de réunion, d'association et syndicale et principe de libre administration territoriale.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Il résulte des dispositions combinées des articles 4 et 115 de la loi du 6 janvier 1978 que des données sensibles ne peuvent être traitées dans le traitement EASP au titre de la préservation de la sûreté de l'Etat que si elles sont nécessaires à la poursuite de cette finalité. En outre, le décret attaqué n'est pas entaché d'illégalité du seul fait qu'il ne rappelle pas que le traitement des données sensibles pour les finalités relevant de la directive 2016/680 du 27 avril 2016 n'est possible qu'en cas de nécessité absolue. Il résulte du dernier alinéa de l'article R. 236-2 et de l'article R. 236-3, d'une part, qu'aucune recherche automatisée ne peut être effectuée à partir des données sensibles et, d'autre part, que ces données ne peuvent provenir que d'un rapport d'enquête administrative, à l'exclusion de toute autre source. Eu égard, en outre, à l'ensemble des garanties fixées par les articles R. 236-4 à R. 236-10 du code de la sécurité intérieure dans leur rédaction résultant du décret attaqué, tenant notamment à la durée de conservation de ces données, aux conditions dans lesquelles les agents mentionnés à l'article R. 236-6 peuvent y accéder ou en être rendus destinataires, à la traçabilité des opérations effectuées dans le traitement et aux droits des personnes concernées définis à l'article R. 236-9, ainsi qu'à l'obligation faite par l'article R. 236-10 au directeur général de la police nationale de présenter chaque année à la CNIL un rapport sur ses activités de vérification, de mise à jour et d'effacement des données enregistrées dans le traitement et indiquant les procédures suivies par les services gestionnaires pour que les données enregistrées soient en permanence exactes, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, notamment pour ce qui concerne les données sensibles, les requérants ne sont pas fondés à soutenir que le traitement litigieux ne serait pas assorti des garanties appropriées exigées par l'article 88 de la loi du 6 janvier 1978.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Articles 8 et 9 de la Convention EDH
- Articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne

➢ CE, 22 juillet 2022, *La Quadrature du net*, n° 451653

(i) Un résumé des faits :

L'article 154 de la loi du 28 décembre 2019 de finances pour 2020 a autorisé à titre expérimental, pour une durée de trois ans, la mise en œuvre, par l'administration fiscale et l'administration des douanes et droits indirects, pour les besoins de la recherche de certaines infractions pénales et de certains manquements susceptibles de donner lieu au prononcé de sanctions administratives en matière fiscale ou douanière, d'un dispositif de collecte et d'exploitation automatisé des contenus librement accessibles sur les sites internet des opérateurs de plateforme en ligne mentionnés au 2° du I de l'article L. 111-7 du code de la consommation. L'association la Quadrature du net demande l'annulation pour excès de pouvoir du décret n° 2021-148 du 11 février 2021 portant modalités de mise en œuvre par la direction générale des finances publiques et la direction générale des douanes et droits indirects de traitements informatisés et automatisés permettant la collecte et l'exploitation de données rendues publiques sur les sites internet des opérateurs de plateforme en ligne.

(ii) La technologie d'IA mise en cause ;

Traitement automatisé de données à caractère personnel

(iii) Les droits humains en question ;

Droit au respect de la vie privée, droit à la liberté de pensée, de conscience et de religion, libertés de réunion, d'association et syndicale et principe de libre administration territoriale.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Il résulte des dispositions combinées des articles 4 et 115 de la loi du 6 janvier 1978 que des données sensibles ne peuvent être traitées dans le traitement EASP au titre de la préservation de la sûreté de l'Etat que si elles sont nécessaires à la poursuite de cette finalité. En outre, le décret attaqué n'est pas entaché d'illégalité du seul fait qu'il ne rappelle pas que le traitement des données sensibles pour les finalités relevant de la directive 2016/680 du 27 avril 2016 n'est possible qu'en cas de nécessité absolue. Il résulte du dernier alinéa de l'article R. 236-2 et de l'article R. 236-3, d'une part, qu'aucune recherche automatisée ne peut être effectuée à partir des données sensibles et, d'autre part, que ces données ne peuvent provenir que d'un rapport d'enquête administrative, à l'exclusion de toute autre source. Eu égard, en outre, à l'ensemble des garanties fixées par les articles R. 236-4 à R. 236-10 du code de la sécurité intérieure dans leur rédaction résultant du décret attaqué, tenant notamment à la durée de conservation de ces données, aux conditions dans lesquelles les agents mentionnés à l'article R. 236-6 peuvent y accéder ou en être rendus destinataires, à la traçabilité des opérations effectuées dans le traitement et aux droits des personnes concernées définis à l'article R. 236-9, ainsi qu'à l'obligation faite par l'article R. 236-10 au directeur général de la police nationale de présenter chaque année à la CNIL un rapport sur ses activités de vérification, de mise à jour et d'effacement des données enregistrées dans le traitement et indiquant les procédures suivies par les services gestionnaires pour que les données enregistrées soient en permanence exactes, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, notamment pour ce qui concerne les données sensibles, les requérants ne sont pas fondés à soutenir que le traitement litigieux ne serait pas assorti des garanties appropriées exigées par l'article 88 de la loi du 6 janvier 1978.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Articles 8 et 9 de la Convention EDH
- Articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne

- CAA de Versailles, 10 novembre 2020, *SA La Méridionale*, n° 18VE02707

(i) Un résumé des faits :

Une société ayant fait l'objet d'une vérification de comptabilité critiquait la procédure suivie par l'administration, qui avait recouru à des traitements automatisés de données et à des algorithmes. Elle soutenait que les résultats des traitements opérés par l'administration et les moyens mis en œuvre à cette fin n'avaient pas été portés à sa connaissance. En outre, elle se plaignait de ce que, en l'absence de ces éléments et des algorithmes utilisés pour procéder à ces traitements, elle se trouvait dans l'impossibilité de reconstituer, elle-même, les montants rappelés.

(ii) La technologie d'IA mise en cause ;

Les algorithmes.

(iii) Les droits humains en question ;

Le droit de la défense, le droit à un procès équitable et le principe d'égalité des armes.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Il résulte des articles L. 57 et L. 47 du livre des procédures fiscales que, lorsqu'une société vérifiée choisit, en vertu du c du II de ce dernier article, de mettre à la disposition de l'administration les copies des documents, données et traitements soumis à contrôle, l'administration est tenue de préciser, dans sa proposition de rectification, les fichiers utilisés, la nature des traitements qu'elle a effectués sur ces fichiers et les modalités de détermination des éléments servant au calcul des rehaussements, mais n'a l'obligation de communiquer ni les algorithmes, logiciels ou matériels qu'elle a utilisés ou envisage de mettre en œuvre pour effectuer ces traitements, ni les résultats de l'ensemble des traitements qu'elle a réalisés, que ce soit préalablement à la proposition de rectification ou dans le cadre de celle-ci. Or, après avoir rappelé les fichiers que le vérificateur a utilisés, les propositions de rectification des 17 décembre 2014 et 11 février 2015, décrivent avec précision la nature des traitements effectués et les modalités de détermination des éléments servant au calcul des rehaussements. La circonstance que les tableaux produits par l'administration diffèrent de ceux qui étaient décrits dans la demande de traitement est, à cet égard, sans incidence, dès lors que, ainsi qu'il a été dit au point 3, la demande de traitement informatique a seulement pour objet d'informer le contribuable de la nature des investigations qu'il souhaite effectuer, c'est-à-dire les données sur lesquelles il entend faire porter ses recherches ainsi que l'objet de ces investigations. En outre, contrairement à ce que soutient la requérante, l'administration n'était tenue de lui communiquer ni les algorithmes utilisés, ni l'ensemble des tableaux et résultats des traitements réalisés. En tout état de cause, société LA MERIDIONALE a pu faire valoir ses observations sur ces redressements avant leur mise en recouvrement, par un courrier du 7 avril 2015 auquel, l'administration fiscale a apporté une réponse motivée le 3 juin suivant, il ne résulte pas de l'instruction que la requérante aurait sollicité, à cette occasion, la communication des traitements informatiques opérés et algorithmes employés par l'administration pour établir les redressements en litige. Par suite, les moyens tirés de ce que la procédure suivie a méconnu le principe d'égalité des armes, corollaire de l'article 47 de la Charte des droits fondamentaux, le droit à faire faire valoir ses observations, tel qu'il est prévu par la jurisprudence de la Cour de justice de l'Union européenne, ainsi que les moyens tirés de la méconnaissance des droits de la défense et du droit au procès équitable, doivent être écartés.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

- Article 47 de la Charte des droits fondamentaux de l'Union européenne.

3. <u>Décisions relatives à la responsabilité du fait de résultats produits par les algorithmes</u>

(i) Un résumé des faits ;

Des contentieux ont concerné la fonctionnalité « Google Suggest », intégrée au moteur de recherche de Google.

Cette fonctionnalité suggérait des propositions de requêtes pouvant être considérées comme dénigrantes, par exemple en associant systématiquement au nom d'une personne ou d'un service déterminé le qualificatif d'« escroc » ou « d'arnaque ».

(ii) La technologie d'IA

Des fonctionnalités intégrées à un moteur de recherche

(iii) Les droits humains en question

Le droit à la vie privée et le droit au respect des biens.

(iv) Un résumé du raisonnement et de la décision de la Cour ;

Dans un premier contentieux, la Cour de cassation a écarté la possibilité de retenir la responsabilité de Google sur le fondement de l'article 29 alinéa 2 de la loi du 29 juillet 1889 sur la liberté de la presse, réprimant l'injure (Cass., Civ. 1ère, 19 juin 2013, 12-17.591, au bulletin).

Elle considère, en effet, que « la fonctionnalité aboutissant au rapprochement critiqué est le fruit d'un processus purement automatique dans son fonctionnement et aléatoire dans ses résultats, de sorte que l'affichage des « mots clés » qui en résulte est exclusif de toute volonté de l'exploitant du moteur de recherche d'émettre les propos en cause ou de leur conférer une signification autonome au-delà de leur simple juxtaposition et de leur seule fonction d'aide à la recherche. » En effet, l'injure est un délit supposant la caractérisation d'un élément intentionnel. En l'absence de volonté établie de Google de tenir des propos outrageants, sa responsabilité ne peut être retenue sur ce fondement.

Dans un deuxième contentieux, la Cour de cassation a admis la responsabilité de « Google Suggest» sur le fondement de la violation du droit d'auteur (Cass., Civ. 1ère, 12 juillet 2012, 11-20.538). Elle a considéré que le fait d'orienter systématiquement "*les internautes, par l'apparition de mots-clés suggérés en fonction du nombre de requêtes, vers des sites comportant des enregistrements mis à la disposition du public sans l'autorisation des artistes-interprètes ou des producteurs de phonogrammes", " "offrait les moyens de porter atteinte aux droits des auteurs ou aux droits voisins*".

Dans un troisième contentieux, les juges du fond (voir par exemple, Tribunal de grande instance de Paris, 17e chambre presse - civile, 23 octobre 2013, n° 11/07439) ont pu admettre la responsabilité de Google sur le fondement de la responsabilité civile extracontractuelle pour faute de droit commun (actuel article 1240 du code civil) en raison du défaut d'information et de l'absence de suppression des suggestions.

(v) Toute référence faite par la juridiction nationale aux principes de la CEDH/CSE ou à d'autres normes internationales en matière de droits humains.

Pas de référence à une norme internationale dans ces arrêts.

GEORGIA / *GÉORGIE*

Georgia's domestic courts have not yet issued decisions directly addressing artificial intelligence (AI) and human rights. However, the country's legislative and policy initiatives demonstrate a strong commitment to the principles of human rights, democracy, and the rule of law. Georgia is planning to actively work on the ratification of the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law. This convention provides a robust framework for addressing AI-related human rights concerns in domestic jurisdictions.

GREECE / *GRÈCE*

One case reported:

(i) Facts and details of the technology – sector of activity in which it was applied:

In the Greek legal system, the first case that fully addressed the integration of new technologies, specifically the use of modern automated decision-making systems in the issuance of administrative acts, was examined by the Fourth Section of the Council of State (CoS), with the issuance of Decision No. 1206/2024 (22.1.2024). This case did not involve machine learning or artificial intelligence (AI) systems but broadly the application of electronically automated data processing based on algorithmic calculations, aimed at faster, more efficient, and effective administrative procedures.

Specifically, this case examines the issue of the justification of the Administration's individual administrative acts when they are issued based on an electronic automated process. The facts involved a citizen's application for annulment against the rejection of their proposal for inclusion in the NSRF 2007-2013 program, specifically an application for a grant to purchase specialized design software and modern technological equipment. The electronic evaluation of the proposal resulted in a low score, below the approval threshold, leading to the rejection of the proposal with the issuance of an unfavorable individual administrative act.

The applicant, disputing the decision, submitted an appeal to the Appeals Committee of the Ministry of Economy, Competitiveness, and Shipping, requesting a re-evaluation of their proposal. In their appeal, they cited specific reasons and arguments for correcting the score, claiming that the low score was due to an obvious error. The error, they argued, may have occurred either during the evaluation process of their proposal by the competent committee or during the transfer of their data for electronic processing.

The Administration rejected the appeal, arguing that administrative acts resulting from an automated evaluation process, based on a mathematical formula and objective data, do not require further justification. They claimed that since no human factor is involved in the evaluation and data transfer process, "it is not logical for there to be an error in the calculation." In other words, the Administration argued that there is no need for justification of individual administrative acts issued based on electronic automated data processing because the scientific reliability of the entire process cannot be questioned.

(ii) Specific human rights that are challenged if identified:

The decision is directly linked to the principle of legality and the principle of good administration, which ensures the proper and fair functioning of the administration. Additionally, the decision concerns respect for the guarantees for the unhindered exercise of the constitutionally enshrined right to petition and judicial protection, as provided in Article 20 of the Constitution of the Hellenic Republic. Specifically, it examines the Administration's obligation to justify its individual decisions, which is a fundamental element of the rule of law and is connected to the principles of transparency and legality of administrative action, as well as effective judicial protection, in conjunction with Article 17(1) of the Administrative Procedure Code, which establishes the general rule that individual administrative acts must contain justification, including the determination of the legal conditions for their issuance. Furthermore, the decision focuses on the need to protect the fundamental principles of democracy, such as the Rule of Law and the Principle of Legality of state action.

(iii) *A summary of the domestic court’s reasoning and decision.*

The Council of State found that a simple referral to the algorithm details as they were published in the Call for Applications for the above-mentioned project does not give adequate reasoning for the administrative rejection decision. In the same vein, it rejected claims by the State whereby it was argued that there is no need for specific detailed justification for individual administrative acts when they are issued on the basis of electronic automated data processing, because “it is not logically possible to question the scientific reliability of the entire process” due to the lack of human involvement in it.

According to the Court, the issue that arises, in principle, in the event of a challenge to an individual administrative act issued in whole or in part on the basis of an electronic automated procedure is not related to the technological integrity of the relevant software or hardware used in the relevant procedure, but to the general legality of the administrative act, that is, to the correct interpretation and application of the legal conditions of the legal rule governing its issuance. The obligation of the administration to justify its individual decisions is a fundamental element of the rule of law, closely linked to the principles of transparency and legality of administrative actions, as well as effective judicial protection [enshrined in Article 17, paragraph 1 of the Greek Code of Administrative Procedure (Law 2690/1999, A’ 45). The Court further noted that “this rule has, among other things, the more specific meaning that, in the case of a dispute regarding the legality of an individual administrative act issued wholly or partially based on automated data processing, the decision issued on the relevant objection must disclose both the critical stages of the mathematical calculations carried out by the Authority and the factual elements (variables) that were taken into account. This is to ensure that, on the one hand, the person concerned can determine whether the prescribed legal conditions for its examination were met in their case, and on the other hand, that the judge can effectively exercise the relevant judicial review.”

The decision of the Council of State establishes a clear jurisprudential framework for the use of technology in administrative action, focusing on adherence to the Principle of Legality. Technology is recognized as a tool that can function supportively, aiding decision-making by administrative and judicial bodies. At the same time, technology cannot replace the human factor, especially regarding the processing of vague and evaluative concepts that require legal thinking and specialized analysis.
The Council of State emphasizes that administrative acts issued through automated methods are subject to the same rules of legality as acts based on human intervention. A central element of the legality of these acts is justification, which requires complete and clear documentation of the factual and legal data. According to Article 17 of the Administrative Procedure Code (APC), the absence of justification constitutes a violation of a substantial form, while justification cannot be based solely on mathematical formulas or algorithmic predictions. This rule has, among other things, the specific meaning that in case of questioning the legality of an individual administrative act issued wholly or partly based on automated data processing, the decision must show both the critical stages of the mathematical calculations performed by the Authority and the factual elements (variables) taken into account, so that the governed can determine whether the conditions for its examination were met in their case, and the judge can effectively exercise the relevant judicial review.
The case was referred back to the Appeals Committee for re-examination of the applicant's claims, with the obligation to consider all relevant data and provide full justification.

(iv) Any reference made by the domestic court to the ECHR, ESC or other international human rights standards.

The Council of State does not refer to the ECHR, ESC or other international human rights standards (iv), but it makes reference to comparative law solutions (articles L311-3-1 and R311-3-1-2 of the French Code of Public and Administrative Relations) and jurisprudence (decision 2270 of 8.4.2019 of the Italian Council of State, Consiglio di Stato). It also refers to the relevant provisions of the EU General Data Protection Regulation (in particular Article 22 on the need to ensure, through appropriate measures, "at least the right to ensure human intervention by the data controller, the expression of views, and the possibility to challenge the decision" in favor of the data subject.

ITALY / *ITALIE*

Yes, Italian domestic Courts addressed two main cases involving AI and human rights:

1. Case 14381/2021

In a judgment delivered on 25 May 2021, the Italian Supreme Court addressed the legality of an AI-driven reputational rating system that processed personal data without sufficient transparency or informed consent. The case concerned an undertaking that developed a web platform using algorithms to generate reputational ratings for individuals and businesses. These ratings were calculated by comparing genuine profiles with artificial or fabricated ones and were then offered to third parties as credibility verification tools. The system operated within the area of data analytics and reputation management, with the Italian Data Protection Authority (Garante per la protezione dei dati personali, GPDP) challenging its compatibility with data protection laws.

The human rights at issue were primarily the right to protection of personal data, as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (CFR), and the right to autonomy and freedom in consenting to data processing. The GPDP argued that the opacity of the algorithm undermined users' ability to give informed consent, violating the principles of transparency and autonomy. Additionally, the system raised broader concerns about the fairness and reliability of automated decision-making processes.

The Italian Supreme Court's reasoning focused on the invalidity of consent in the absence of transparency about the algorithm's functioning. Under the Italian Privacy Code, which complements the GDPR, consent for data processing must be informed, freely given, in writing, and specific to a clearly identified purpose. The Court held that the inherent opacity of the algorithm made it impossible for individuals to understand how their data was being used or how reputational ratings were derived. As a result, any purported consent to data processing was invalid. The Court rejected the lower Court's argument that such transparency issues could be left to market forces, affirming that regulatory oversight is necessary to protect individual rights.

The Court explicitly referenced Article 7 of the GDPR, which governs the validity of consent, and Recitals 32 and 33 of the GDPR, which emphasize the need for clarity in obtaining consent. While the judgment primarily applied European data protection standards, it indirectly engaged with international human rights frameworks, such as the European Convention on Human Rights (ECHR), through its reliance on Article 8 of the CFR, a document aligned with the ECHR in protecting fundamental rights.

By prohibiting the use of opaque algorithms to process personal data for reputational purposes, the judgment reinforces the principle that AI systems must meet stringent transparency and accountability standards to comply with human rights and data protection laws.

2. Case 2270/2019

The Italian Council of State addressed the use of algorithmic decision-making in public administration, particularly focusing on a case involving the automated assignment of secondary school teachers. The Ministry of Education employed an algorithm within a web-based platform to manage the national mobility procedure for teachers, aiming to allocate positions based on preferences and rankings. However, the process resulted in several anomalies:

- Teachers were assigned to subjects they had never taught.
- Assignments did not align with the preferences expressed by the teachers.
- Many teachers were placed in provinces far from their original locations.

The affected teachers contested these outcomes, arguing that the algorithm's operations were opaque and lacked transparency. They highlighted the absence of clear reasoning behind the assignments and the inability to identify any administrative official responsible for evaluating individual cases. This, they claimed, violated principles of impartiality, transparency, and the right to a reasoned decision.

While recognizing the benefits of digitalization and the use of algorithms in enhancing efficiency within public administration, the Council of State emphasized that such tools must adhere to fundamental administrative principles. The Court found that the opacity of the algorithm breached the principles of impartiality, publicity, and transparency, as it was impossible to understand the criteria and methods used for the assignments. Additionally, the illogical and irrational outcomes of the procedure underscored the need for human oversight in algorithmic decision-making processes.

While the judgment did not explicitly reference international human rights instruments such as the European Convention on Human Rights (ECHR) or the European Social Charter (ESC), it underscored the necessity for transparency, accountability, and the right to a reasoned decision in administrative procedures. These principles align with broader international human rights standards that advocate for fairness and transparency in automated decision-making.

LATVIA / *LETTONIE*

At present, there are no domestic case law examples that specifically address the relationship between artificial intelligence (‘AI’) and human rights or the possible implications of AI on the human rights in Latvia.

At the same time, in two domestic court proceedings the courts have used AI technology during the proceedings or provided some considerations as to the wider development of technologies and their potential impact on the obligations of State to continuously improve the domestic legal framework.

1.1. In the first example, a simulation provided by the AI system *ChatGPT* was used by the defence during criminal proceedings.

Person X was charged with committing a criminal offence stipulated in Article 262[1], paragraph 1, of the *Criminal Law* (as in force until 4 July 2024). The criminal case concerned the refusal of the driver to undergo testing for narcotic, psychotropic, toxic, or other intoxicating substance level in blood, since the accused person claimed that they were not driving the vehicle at the relevant time.

During a court hearing, the court examined results of a simulation produced by the AI system *ChatGPT*, demonstrating the shortest possible time for person Y to move to the back seat of the car and for person X to take the driver's seat, which was submitted by defence. The same simulation was again conducted during the court hearing, using more precise input data, including the model of the car and the specifications of the individuals involved – their age, weight, and height. The AI system *ChatGPT* ultimately established that:

> "[..] considering the driver's height, the complexity of leg and upper body movements, and the required synchronization with the passenger, the total minimum time for both individuals to fully switch seats would be approximately 7-9 seconds."

Although the *Criminal Procedure Law* does not explicitly address the use of AI in proving whether a criminal offence has been committed, the court recognised the right of the defence to present evidence that may indicate whether the actions carried out by the accused could or could not have been considered as a criminal offence. The court further acknowledged that the simulation results provided by the AI system in question, as examined during the court hearing, suggested the possibility that the testimony of person X was truthful and that the described switching of seats in the vehicle was possible. The court found person X not guilty of committing the criminal offence stipulated in Article 262[1], paragraph 1, of the *Criminal Law* (as in force until 4 July 2024). However, it should be noted that the ruling of the court has not yet entered into force as the prosecutor has appealed against it.

1.2. In another case before the Constitutional Court of the Republic of Latvia, which did not pertain specifically to AI, the Constitutional Court provided a forward-looking *obiter dictum*, which, to some extent, might be applicable to AI, as well. In the case no.2017-30-01[3] the Constitutional Court examined the compatibility of a provision of the *Civil Procedure Law* according to which plaintiffs in civil cases had to indicate the "declared" (registered) place of residence[4] of the defendant, failing which the civil suit is liable to be dismissed. An individual asked the competent authority to disclose the declared place of residence of several public persons (the Prime Minister, *etc*.), alleging a wish to file a civil suit against those persons. The refusal of the competent authority to disclose that information was appealed in administrative courts, and the Supreme Court eventually disputed the constitutionality of the specific provisions of the *Civil Procedure Law* before the Constitutional Court, arguing that they were contrary to the right to respect for one's private life, which is protected by Article 96 of the *Constitution*.[5]

The Constitutional Court held that the contested provisions of the *Civil Procedure Law* constituted a restriction of (or an interference with) the right to respect for one's private life. It

[3] The judgment of the Constitutional Court of 11 October 2018 in the case no.2017-30-01, available in English at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2017/11/2017-30-01_Judgment.pdf.

[4] Every person in Latvia has an obligation to declare an address in which they may be reached for purposes of official correspondence.

[5] **Article 96**
Everyone has the right to inviolability of his or her private life, home and correspondence.

found that the restriction was prescribed by law and pursued a legitimate aim – the protection of rights of others (in the specific case it was found that indicating the declared place of residence was necessary to establish the competent court and also to ensure that the eventual defendants would be correctly served with the procedural documents). The Constitutional Court dismissed the argument that indicating a person's place of employment instead of their place of residence would be a suitable alternative to the contested regulation. Neither did the Constitutional Court consider that placing an obligation to establish the defendant's address on the court, which has received the civil suit, could be considered a suitable alternative.

After ascertaining that a similar regulation was in place in a significant number of other European states and after having established that the Latvian legal system provided for sufficient guarantees against potential abuse of the system of requesting information on potential defendant's place of residence, the Constitutional Court found the restriction of the right to respect for one's private life to be proportionate. Thus, the contested regulation was found to be constitutional.

However, after having concluded the examination of the case on the merits, the Constitutional Court included in the judgment an *obiter dictum*, which might be of future relevance when encountering issues related to, *inter alia*, the use of AI:

> "[..]the Constitutional Court draws attention to the fact that as a result of the rapid development of information technologies, the possibilities of courts to access various databases have also significantly expanded, while the regulation included in the contested provisions regarding the role of the court in civil proceedings has not changed in its essence for a certain period of time. The Constitutional Court has already noted many times that the legislator is obliged to periodically consider whether a given legal regulation is still effective, appropriate, and necessary and whether it should be improved in any way [..]. The evolution of technology, the judicial system, and legal relations between members of the society can make legal frameworks that were once in conformity with higher-ranking legal rules obsolete and ultimately even violate fundamental personal rights."

The judgment includes multiple and detailed references to the Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights. However, these are references that focus on the protection of personal data and other matters, not the impact of technologies on fundamental rights.

LIECHTENSTEIN

No.

LITHUANIA / *LITHUANIE*

At present, the classifiers in the Lithuanian Court Information System do not include a specific code for identifying cases or court decisions related to artificial intelligence and human rights.
Automated searches in the Lithuanian Court Information System are also possible using keywords, such as the names of legal acts regulating the use of artificial intelligence applied in cases. However, after conducting such a search, no cases addressing artificial intelligence were found.

MALTA / *MALTE*

No reply.

MONACO

Non.

MONTENEGRO / *MONTÉNÉGRO*

The domestic courts in Montenegro have not yet addressed any cases involving artificial intelligence and human rights.

NETHERLANDS / *PAYS-BAS*

Our domestic courts have dealt with cases involving automated systems, or laws applying to the use of automated systems. In none of those cases the court made the official determination whether AI as defined by EU law or the CoE Convention on AI was used, as both legal instruments were not in force yet. However, the cases cited below may be relevant to the use of AI and human rights.

The SyRI Case[6]

In the Dutch SyRI case, the Hague District Court delivered a judgement that SyRI legislation was in breach of the European Convention on Human Rights. Systeem Risico Indicatie, or SyRI, is a legal instrument used by the Dutch government to detect various forms of fraud, including social benefits, allowances, and taxes fraud. The court has ruled that the legislation regulating the use of SyRI violates higher law. The court has decided that this legislation does not comply with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home, and correspondence.

Several civil society interest groups, including the Dutch Section of the International Commission of Jurists (NJCM) and two private individuals, instituted these proceedings against the State of the Netherlands. The Netherlands Trade Union Confederation (FNV) joined as a party in the claimants' proceedings. Claimants want to call 'a halt' to the use of SyRI. They believe that by applying SyRI, the Netherlands government unlawfully violates human rights. The State disagrees and argues that the SyRI legislation contains sufficient safeguards to protect the privacy rights of all.

Although the court did not judge on whether big data or AI was used it did consider: "There currently are no indications of 'deep learning' or data mining or the development of risk profiles in the implementation of the SyRI legislation. However, the SyRI legislation does provide scope for the development and application of a risk model using 'deep learning' and data mining, and for the development of risk profiles." (see 6.63)

(i) Summary of the Facts:
The *Systeem Risicoindicatie* (hereinafter: SyRI) is a legal instrument the Netherlands government uses to prevent and combat fraud in social security and income-dependent schemes, taxes and

[6] See: ECLI:NL:RBDHA:2020:1878, Rechtbank Den Haag, C-09-550982-HA ZA 18-388 (English)

social security, and labour laws. According to the legislator, SyRI is a technical infrastructure with associated procedures with which data can be linked and analysed anonymously in a secure environment, so that risk reports can be generated.

(ii) Specific Human Rights at Issue:
The case raised concerns about several human rights issues, particularly:

- Right to privacy (Article 8 of the ECHR)
- Right to a fair trial (Article 6 of the ECHR)
- Right to a remedy (Article 13 of the ECHR)

(iii) Summary of the Domestic Court's Reasoning and Decision:

The court reviewed whether the SyRI legislation is in breach of provisions of international or European law binding on all persons. The court assessed whether the SyRI legislation complies with Article 8 paragraph 2 ECHR. This particular provision requires striking a fair balance between the interests of the community, which the legislation serves, and the right of the individuals affected by the legislation to respect for their private life and home.

According to Article 8 ECHR the Netherlands – as a party to the ECHR – has a special responsibility when applying new technologies. It must strike the right balance between the benefits such technologies bring and the violation of the right to a private life using new technologies. This also applies to the use of SyRI.

After a review of the objects of the SyRI legislation, namely preventing and combating fraud in the interest of economic welfare, in relation to the violation of private life by the legislation, the court has drawn the conclusion that in its current form the SyRI legislation fails to comply with Article 8 paragraph 2 ECHR. The court has decided that the legislation does not strike a fair balance, as required under the ECHR, which would warrant a sufficiently justified violation of private life. In that respect, the application of SyRI is insufficiently transparent and verifiable. As such, the SyRI legislation is unlawful, because it violates higher law and, as a result, has been declared as having no binding effect.

Because of its lack of transparency, the court did not assess whether the SyRI legislation was contrary to one or more specific provisions of the GDPR brought forward by the partyies, and whether the SyRI legislation was in violation of Articles 6 and 13 ECHR. The court therefore leaves undiscussed the other arguments and defences of the parties.

(iv) References to International Human Rights Standards:
The Dutch court referred to the European Convention on Human Rights (ECHR).

The PAS/Aerius case[7]

(i) Brief Summary of the Facts
The case involves the granting of permits by the College of Deputies of North Brabant on December 14, 2015, under Article 16 and 19d of the Nature Conservation Act 1998. These permits were for the operation, expansion, and modification of six agricultural businesses. The Stichting Werkgroep Behoud de Peel (Foundation Group to Preserve the Peel) challenged these permits, leading to the case being brought before the Raad van State (Council of State).

[7] ECLI:NL:RVS:2017:1259, Raad van State, 201600614/1/R2, 201600617/1/R2, 201600618/1/R2, 201600620/1/R2, 201600622/1/R2 en 201600630/1/R2

(ii) Specific Human Rights at Issue
The case primarily dealt with environmental protection. However, the court raised important points on transparency in administrative decisions and equality before the law.

(iii) Domestic Court's Reasoning and Decision
The court upheld the permits but emphasized the need for transparency and accountability in the (partly automated) decision-making process.

Specifically, the court said, that without transparency on the model used to reach an administrative decision, if interested parties wish to use legal remedies against decisions based on the model, this may result in an unequal procedural position of the parties. In the case of decision-making based on a program that from their perspective can be regarded as a so-called "black box", they cannot check on the basis of which a certain decision is reached.

Notably, it said that to prevent this unequal procedural position, the aforementioned Ministers and the State Secretary are obliged in this case to make the choices made and the data and assumptions used public so that these choices, data and assumptions are accessible to third parties. This will ensure that legal protection against decisions based on these choices, data and assumptions is possible.

(iv) References to International Human Rights Standards
The domestic court did not make specific references to the European Convention on Human Rights (ECHR) or other international human rights standards.

The child benefits scandal[8]

The child benefits scandal has been a much-cited scandal involving the use of automated technologies. Although there have been many court cases, none of them evaluate the risk assessment tool specifically. However, the data protection authority has issued a decision on it. The cited document is its investigation into the Dutch childcare benefits scandal involving the Dutch Tax Authority (Belastingdienst/Toeslagen).

(i) Brief Summary of the Facts
The Dutch childcare benefits scandal (Toeslagenaffaire) centered around the misuse of technology and data processing in the administration of childcare benefits. The Belastingdienst employed algorithms, including risk classification models, which used sensitive personal data like nationality to flag "high-risk" applications for fraud investigations.

Applicants with foreign or dual nationalities were disproportionately targeted, leading to discriminatory practices. Many were unfairly labeled as fraudsters, resulting in significant financial harm as they were forced to repay benefits without proper justification.

(ii) Specific Human Rights at Issue
The case implicated several human rights issues, including:

1. General prohibition of discrimination (Artikel 1 of Protocol nr. 12 ECHR, 26 International Covenant on Civil and Political Rights)
2. Right to Privacy (Article 8 ECHR, although this case cites the EU GDPR mostly).

[8] https://www.autoriteitpersoonsgegevens.nl/documenten/onderzoek-belastingdienst-kinderopvangtoeslag

(iii) Summary of the Domestic Court's Reasoning and Decision
The Data Protection Authority (AP) found that the tax office violated both national and EU data protection laws, particularly the General Data Protection Regulation (GDPR). The AP highlighted the lack of necessity and proportionality in collecting nationality data and using it as a criterion in the risk classification models.

The authority also investigated the lawfulness of the data processing practices by the Belastingdienst. It considered two processing activities as discriminatory practices, notably the use of nationality as an indicator in the risk model, as they lacked an objective justification for the use of nationality data in the model.

(iv) References to International Human Rights Standards
The investigation referenced the ECHR, EU data protection law, and the International covenant on civil and political rights.

DUO case on automated risk profiling[9]

The District Court of Overijssel addressed the use of automated decision-making by the Dienst Uitvoering Onderwijs (DUO) in selecting students for verification of their eligibility for the "out-of-home" student grant.

(i) Summary of the Facts
DUO employed an automated risk profiling system to identify students who might falsely claim to live independently to receive higher financial aid. This (simple) system analyzed various data points, including the distance between students and their parents' home and their age to flag cases for further investigation. One student was denied financial aid, after such an investigation led investigators to believe she didn't live independently.
(ii) Specific Human Rights at Issue
The case raised concerns about indirect discrimination, particularly regarding the potential for the automated system to disproportionately target certain groups of students.

(iii) Summary of the Domestic Court's Reasoning and Decision
The court found that DUO's use of the automated risk profiling system led to indirect discrimination. The system disproportionately selected students from specific backgrounds for verification without sufficient justification. Consequently, the court ruled that evidence obtained through this discriminatory process was inadmissible, and DUO was required to cease using the flawed profiling system.

(iv) References to International Human Rights Standards
The court referenced Article 14 of the ECHR, which ensures the right to non-discrimination in the enjoyment of rights and freedoms set forth in the Convention. Additionally, the court considered Article 1 of Protocol No. 12 to the ECHR, which provides a general prohibition of discrimination.

Predictive policing case in Rotterdam[10]

[9] ECLI:NL:RBOVE:2024:5627, Rechtbank Overijssel, ak_23_1340 en ak_23_1341
[10] ECLI:NL:GHDHA:2021:2586, Gerechtshof Den Haag, 200.297.639/01

The Court of Appeal of The Hague examined the legality of the police's authority to search individuals labeled as "safety risk subjects" (veiligheidsrisicosubjecten) in the context of combating excessive violence.

(i) Summary of the Facts
To combat excessive crime in the city of Rotterdam, the police employed an automated system to designate certain individuals as safety risk subjects, based on data analysis. Once designated as a safety risk subject, these individuals would be subjected to preventive searches without immediate suspicion, aiming to mitigate risks associated with excessive violence.

(ii) Specific Human Rights at Issue
The case raised concerns regarding:

- Right to Privacy (Article 8 of the European Convention on Human Rights - ECHR)
- Right not to be tried or punished twice (Article 4 of Protocol No 7 to the ECHR)

(iii) Summary of the Domestic Court's Reasoning and Decision
The Court of Appeal determined that the procedure formed an interference of the right to privacy, for a suitable goal, but that this was not sufficiently provided for by law. The legal authority to conduct searches on individuals solely based on their designation as safety risk subjects without specific suspicion for a such an extended period of time, based on a past score was insufficiently specific. The court emphasized that such practices could violate individuals' rights to privacy.

(iv) References to International Human Rights Standards
The court referenced:

- Article 8 ECHR: Highlighting the right to respect for private and family life, the court noted that unwarranted searches infringe upon this right.

Proctoring case[11]

The Amsterdam District Court examined the University of Amsterdam's (UvA) use of online proctoring software during examinations necessitated by the COVID-19 pandemic.

(i) Summary of the Facts
Due to COVID-19 restrictions, UvA implemented online proctoring software to conduct remote examinations, aiming to maintain academic integrity. This software utilized students' webcams to monitor their behavior during exams, employing algorithms to detect potential fraud by flagging unusual activities, such as looking away from the screen. The proctoring system recorded video data, which was encrypted and stored on EU-based servers, accessible only to authorized UvA staff.

(ii) Specific Human Rights at Issue
The court identified concerns related to:

- Right to Privacy (Article 8 of the European Convention on Human Rights - ECHR): The use of online proctoring involved processing personal data, including video recordings of students in their private spaces, raising privacy issues.

(iii) Summary of the Domestic Court's Reasoning and Decision
The court ruled that UvA's use of online proctoring was lawful under the circumstances, emphasizing the following points:

[11] ECLI:NL:RBAMS:2020:2917, Rechtbank Amsterdam, C/13/684665 / KG ZA 20-481

- Necessity: Given the COVID-19 restrictions, in-person examinations were not feasible. Online proctoring was deemed necessary to fulfill UvA's legal obligation to ensure the quality and integrity of examinations.
- Data Protection Measures: UvA conducted a Data Protection Impact Assessment (DPIA) and implemented safeguards, such as data encryption, limited data retention (30 days), and restricted access to authorized personnel, aligning with GDPR requirements.
- Proportionality: The court found that the measures taken were proportionate to the aim of preventing fraud, considering the temporary nature of the solution and the public interest in maintaining educational standards.

(iv) References to International Human Rights Standards
The court referenced the EU General Data Protection Regulation (GDPR): Emphasizing compliance with data protection principles, particularly regarding the processing of personal data and conducting a DPIA.

POLAND / *POLOGNE*

To date, a few domestic judgments have been recognised in this area. An example is the decision of the Bydgoszcz District Court of 17 December 2024 (ref. no. V NKD 227/24). In the statement of facts, two teenagers from Bydgoszcz used Artificial Intelligence (AI) tools to alter a photograph of a female friend so that she looked in it as if she was naked. In the court's view the minors showed signs of demoralisation and, on the basis of the Act on Support and Rehabilitation of Minors, the court issued them with a warning. The teenagers apologised to their friend.

SAN MARINO / *SAINT-MARIN*

No.

SERBIA / *SERBIE*

No, domestic courts have not yet addressed any cases involving artificial intelligence and human rights.

SLOVAKIA / *SLOVAQUIE*

In the Slovak Republic, the required information is not collected in an official manner.

Anyway, at this time, we do not have any information regarding cases in our country’s domestic courts that specifically address artificial intelligence and human rights.

SPAIN / *ESPAGNE*

Regarding this question, we conducted an exhaustive search for rulings related to artificial intelligence and human rights in Spain. To date, there are no court rulings explicitly addressing cases involving artificial intelligence in the context of human rights.

However, we identified indirect references in cases related to fundamental rights, such as privacy, non-discrimination, and equality. These references are primarily focused on data protection and

do not include specific analyses of artificial intelligence algorithms, rendering them irrelevant to the scope of this inquiry.

As an exception, we found a ruling by the High Court of Justice of Madrid, Administrative Chamber, Judgment No. 139/2022, dated February 4, 2022. This case examined whether a project qualifies as artificial intelligence for tax deduction purposes, explicitly mentioning the use of AI techniques like Bagging and Boosting in developing a predictive model. However, this case does not directly address human rights.

SWITZERLAND / *SUISSE*

Swiss Federal Supreme Court12

The Swiss Federal Supreme Court addressed this issue in its ruling of 17 October 2024 (case no. 1C_63/2023), which examined several newly introduced provisions in the Police Act of the Canton of Lucerne (PolG/LU). The provisions in question contemplated the use of automated data processing and analysis systems, including technologies that could involve artificial intelligence (AI). These provisions raised significant human rights concerns, particularly in relation to privacy, data protection, and the potential for algorithmic discrimination. While none of the provisions contemplated the use of AI systems explicitly, they did not exclude such use.

(i) Brief Summary of the Facts and the AI Technology

The case stemmed from amendments to the Police Act of Lucerne, which introduced provisions that allowed the police to use various forms of automated surveillance and data analysis. Specifically, the amendments permitted notably the use of automated vehicle surveillance systems (§ 4quinquies), the operation of data analysis systems for serial crime (§ 4sexies), and a broad police information system network for data exchange among federal and cantonal authorities (§ 4octies). Some of these provisions permitted the automated processing of large amounts of personal data, including vehicle and individual identification, which could involve AI-driven facial recognition, profiling, and predictive policing techniques.
The Swiss Federal Supreme Court was asked to assess whether these provisions complied with Swiss constitutional guarantees, particularly regarding the right to privacy (Article 13 of the Swiss Constitution), and whether they adhered to international human rights norms, including the European Convention on Human Rights (ECHR).

(ii) Specific Human Rights at Issue

The main human rights at stake in this case were the right to privacy, including issues of protection of personal data (Article 8 ECHR). The plaintiffs also raised concerns about the potential for automated surveillance systems to undermine the right to a fair trial and the presumption of innocence (Article 6 ECHR), particularly in cases where individuals might be subject to unwarranted suspicion or discrimination due to errors in AI-based systems. Lastly, they raised concerns as to the right to an effective remedy (Art. 13 ECHR).

(iii) Summary of the Court's Reasoning and Decision

In its decision, the Swiss Federal Supreme Court found that certain provisions of the amended Police Act violated constitutional and human rights standards, while others were upheld, subject to strict interpretation. Here is a summary of the main considerations.

[12] Decision 1C_63/2023 of 17 October 2024, available here (in German). A summary in French is available here: https://swissprivacy.law/334/

Automated Vehicle Surveillance (§ 4quinquies): The Court ruled that this provision was unconstitutional and struck it down. It found that the mass, non-targeted surveillance allowed under this provision, which included the automated capture of vehicle license plates and passenger images, was a severe infringement on the right to privacy. The law failed to establish sufficiently clear and precise limits on data collection and retention, making it disproportionate. The Court emphasized that such broad surveillance measures must be narrowly defined by law to comply with Article 8 of the ECHR. In its reasoning, the Court also referred to the ECtHR decision *Centrum för Rättvisa v. Sweden* from 25 May 2021, noting that indiscriminate data collection could deter individuals from exercising their rights freely. This provision was also struck down as issues of criminal procedure, such as tracking suspects in an ongoing investigation, is a federal competence, not a cantonal one.

Analysis Systems for Serial Crime (§ 4sexies): The provision authorized the police to use systems for the analysis of patterns and trends in serial crime data (theft, break-ins, shoplifting, arson, etc.). While the statute's drafting history showed that the systems considered were more akin to manually updated databases, the statute itself did not exclude the use of AI-driven systems. The Court upheld this provision but only under a **strict interpretation**. It clarified that the use of data analysis systems for detecting serial crime could be permissible as long as the systems used were not highly complex or predictive. Accordingly, the provision was upheld as long as it was interpreted as excluding the use of AI or automatic facial recognition. In addition, the Court indicated that permissible analysis systems must be explicitly mentioned in the ordinance or in the list of data processing activities of the police in order to ensure transparency and legal certainty.

Information System Network (§ 4octies): The Court struck down this provision, stating that it allowed for the blanket exchange of police data among various cantons and federal authorities without sufficient regulation or safeguards. The lack of clear limits on the categories of data that could be exchanged and the purposes for which it could be used rendered the provision unconstitutional.

(iv) References to the ECHR or Other International Standards
Article 8 ECHR (right to privacy) was central. The Court also noted potential relevance of Articles 6 and 13 ECHR for fair trial and effective remedies.

Civil Court of the canton of Basel (1st instance)
This case was reported in the press, but the decision was not published. Shortly before the 2022 national elections, one member of the Swiss Parliament (A) posted a deepfake video of another member of the Swiss Parliament (B) on X and Instagram. In it, B called for people to vote for A's party and for foreign criminal offenders to be deported. On 17 October 2023, the Civil Court of the canton of Basel ruled that posting this fake video constituted a violation of B's personality rights. A was ordered to pay the court costs and compensation to B, amounting to around CHF 4,000. The ruling is final. However, both parties have waived the right to a statement of reasons. Accordingly, it is unclear whether the court referred to the right to privacy as guaranteed by Article 13 of the Federal Constitution, and even less so whether they relied on the ECHR. As far as we are aware, B has also filed a criminal complaint, but no decision has been rendered yet in this second case.

Recruiting dispute settled in a pre-trial conference13
The Federal Commission for Women's Issues regularly publishes a specialist magazine on questions of gender equality. In an issue dedicated to the impact of AI and algorithms on gender equality, a lawyer reported on a recent domestic case he had been involved in. The plaintiff, an experienced employee in the marketing sector, had applied to a job at another company who had announced that the recruiting process would involve multiple tests, including a psychological assessment tool supported by AI. Her application was rejected at an early stage of the process and she later found out that a man who was, in her opinion, less experienced, had been hired in her stead. During the pre-trial stage, the company agreed to submit the tool to a test devised by the plaintiff's lawyer. The tool turned out to favour male candidates under certain circumstances. The company who had developed the bespoke tool subsequently also investigated its software and confirmed that there was bias. The case was settled before going to trial. As such, no decision was rendered.

TÜRKIYE

No reply.

UNITED KINGDOM / *ROYAUME-UNI*

In 2019, a case related to the use of Automated Facial Recognition (AFR) by a Police Force was brought to the UK court. The Police Force ran a pilot phase to trial the use of AFR, which involved deploying surveillance cameras to capture digital images of members of the public, which were then processed and compared with images of persons on police watchlists. If no match was made, the image was immediately and automatically deleted.

The Claimant challenged the lawfulness of the Police Force's use of AFR. The Claimant was present on two occasions when AFR was being used in a public place. The first time, AFR was deployed on a street in the city centre, primarily to locate and detain wanted "Priority and Prolific Offenders". The Claimant stated they were in range of the cameras used for AFR and did not see signage or any warning that AFR was in use.

On the second occasion, AFR was deployed during an Exhibition as during previous years the event had attracted disorder. The Claimant stated that they attended a protest outside the venue and prior to seeing the AFR-equipped van, was not aware that AFR was in use.

The Claimant contended that the use of this AFR was contrary to Convention rights, the requirements of data protection legislation, and public-sector equality duty. Under the Convention claim, it was contended that using AFR was an interference with their rights under Article 8 as the interference was neither "in accordance with the law" nor "necessary" or "proportionate". On data protection, the Claimant contended that the Police Force failed to act in accordance with the principles set out in the Data Protection Act (DPA) 1998/2018. The Claimant also contended that the Police Force failed to comply with the obligation on public authorities to have "due regard" to

[13] Details as to this case can be found here:
https://www.ekf.admin.ch/dam/ekf/fr/dokumente/zeitschrift/PDFsFrauenfragen2024/FF_2024_david_raedler.pdf.download.pdf/FF_2024_david_raedler.pdf

certain prescribed matters when exercising their function (section 149(1) of the Equality Act 2010). This was in relation to the equality impact assessment document created by the Police Force in respect of its proposed use of AFR. The Claimant contended that the assessment failed to take into consideration the possibility that the use of AFR software would produce a disproportionately higher rate of false positive matches for women and persons from minority ethnic groups, resulting in AFR indirectly discriminating against those groups.

The first instance Court found that while the use of AFR did entail interference with Article 8(1), they were satisfied the Police Force's use of AFR had been consistent with the requirements of Article 8 and the data protection legislation, and that the current legal framework was adequate to ensure appropriate and non-arbitrary use of AFR. The claim was dismissed on all grounds.

The Claimant appealed this decision on five Grounds:

1. The Court erred in concluding that the interference with their rights under Article 8 was in accordance with the law
2. The Court made an error of law in assessing whether the Police Force's use of AFR constituted a proportionate interference with Article 8 rights
3. The Court was wrong to hold that the Police Force's Data Protection Impact Assessment complied with the DPA 2018.
4. The Court erred in declining to reach a conclusion as to whether the Police Force had an appropriate policy document which complies with the requirements of Section 35(5) of the DPA 2018.
5. The Court was wrong to hold that the Police Force complied with the public-sector equality duty

The appeal was subsequently allowed on Grounds 1, 3 and 5. Grounds 2 and 4 were rejected. The Court of Appeal reached the conclusion that there were "fundamental deficiencies" in the legal framework and the Police Force's use of AFR breached privacy rights, data protection laws and equality laws. More specifically:

1- Interference with the Claimant's Article 8 rights was not "in accordance with the law". There was no clear guidance on where AFR could be used and who could be put on a watchlist. There was too broad a discretion to afford to police officers to meet the standard required by Article 8(2).
2- Had the interference with Article 8 been in accordance with the law, it would have been a proportionate interference. The first instance court had properly performed the correct balancing exercise of relevant factors.
3- The data protection impact assessment was inadequate. It was written on the basis that Article 8 was not infringed, when the impermissibly wide areas of discretion meant it was infringed. The impact assessment failed to properly assess the rights and freedoms of data subjects and failed to address the measures envisaged to mitigate the risks arising from the identified deficiencies.
4- The data processing was "sensitive processing" within the meaning of the data protection legislation, which meant that the police had to have an appropriate policy document in place meeting specific statutory criteria. The first instance court had been correct to

conclude that it did not need to determine the adequacy of the policy document because the AFR was used before the relevant statutory requirement was in force.

5- The first instance court had been wrong to find that the police force had done all it reasonably could to fulfil its public sector equality duty. The duty was important to ensure that a public authority did not inadvertently overlook the potential discriminatory impact of a new, seemingly neutral policy. The police force had never investigated whether AFR had an unacceptable bias on grounds of race or gender. The fact that the technology was being piloted made no difference to the duty on the police force.

UKRAINE

To date, Ukrainian jurisprudence lacks precedential decisions addressing artificial intelligence and human rights. However, we provide an overview of the relevant case law from the Supreme Court regarding the use of artificial intelligence in court proceedings.

On 8 January 2024, the Supreme Court, upon considering the application of the plaintiff's representative in case No. 925/200/22, issued a ruling in which it expressed its position on the use of artificial intelligence by trial participants.

In particular, the plaintiff's representative asked the Supreme Court to clarify certain concepts and conclusions contained in the Supreme Court's ruling of 1 December 2023, which was issued following consideration of the plaintiff's cassation appeal in this case. To justify the need for relevant clarifications, the applicant cited the provisions of certain articles of the Civil Code of Ukraine, the provisions of the textbook ‘Civil Law’, as well as the meaning of the concept of ‘voluntary obligation’ provided by ChatGPT.

The Supreme Court recognised the plaintiff's representative's application for clarification of the Supreme Court's ruling of 1 December 2023 in case No. 925/200/22 as an abuse of procedural rights and left the application without consideration.

In the aforementioned ruling, the Supreme Court, referring to international standards for the use of artificial intelligence in the field of justice, stated that as of today, Ukraine has not approved ethical standards and norms governing the use of artificial intelligence in the judiciary, and has not defined the limits (ethical, legal) of the use of artificial intelligence systems for the purposes of providing professional legal assistance, which, according to the Concept for the Development of Artificial Intelligence in Ukraine, is one of the tasks of state policy in the field of legal regulation of the artificial intelligence industry.

The use of technology must first and foremost respect the nature of the judicial process. Technology should not interfere with the sphere of justice. Therefore, technological tools should respect the judicial decision-making process and the autonomy of judges (paragraph 90 of the Consultative Council of European Judges Opinion No. 26 (2023) “Moving forward: the use of assistive technology in the judiciary”).

In addition, the Supreme Court found that artificial intelligence can be a useful and auxiliary tool in the field of justice, but cannot replace the role of judges. Technology should only be used to support and enhance the rule of law. Technology may only be used to support and assist courts and judges in the proper management and determination of proceedings.

QUESTION 2

ENGLISH

Has your country implemented any specific measures, guidelines, or practices which aim to address potential impacts on human rights by businesses involved in the artificial intelligence systems lifecycle[14], and to provide remedies when such impacts occur?

If so, please provide details, including:

(i) The legal or policy frameworks in place, including specific obligations or guidelines aligned with international standards (e.g., UN Guiding Principles, OECD Guidelines) for businesses to address human rights risks across the AI lifecycle.
(ii) Mechanisms for monitoring and assessing business compliance with human rights standards in the context of AI, and mechanisms through which rights holders may seek remedies.
(iii) Examples of practices that enable corporate responsibility to respect human rights[15] and meaningful stakeholder engagement in the context of AI (for e.g. advisory forums or regular meetings)[16].
(iv) Any sector specific measures, guidelines, or practices concerning the following public governance sectors[17]:

- Law Enforcement and Public Safety
- Administration of Justice
- Healthcare
- Education
- Social Services and Welfare
- Immigration and Border Control
- Labour and Employment
- Housing and Urban Planning
- Taxation
- Democratic Processes
- Public Administration

FRENCH

Votre pays a-t-il mis en œuvre des mesures, des lignes directrices ou des pratiques spécifiques visant à traiter les impacts potentiels sur les droits humains des entreprises impliquées dans le cycle de la vie des systèmes d'intelligence artificielle,[18] et à fournir des recours lorsque de tels impacts se produisent ?

[14] Regarding activities within the lifecycle of artificial intelligence systems see §§ 14-15 of the Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, "without giving an exhaustive list of activities within the lifecycle which are specific to artificial intelligence systems, the Drafters aim to cover any and all activities from the design of an artificial intelligence system to its retirement, no matter which actor is involved in them".

[15] See Section III of the Appendix to Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business.

[16] See as an example Article 67 (Advisory Forum) of Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (EU AI Act) concerning the establishment of an advisory forum.

[17] For further details on the listed public governance sectors, see document CDDH-IA(2024)06REV.

[18] *En ce qui concerne les activités au cours du cycle de vie des systèmes d'intelligence artificielle, voir les paragraphes 14-15 du rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, « sans donner de liste exhaustive des activités menées dans le cadre du cycle de vie qui sont spécifiques aux systèmes d'intelligence artificielle, les rédacteurs visent à couvrir toutes les activités*

Dans l'affirmative, merci de fournir des détails, notamment sur :

(i) Les cadres juridiques ou politiques en place, y compris les obligations spécifiques ou les lignes directrices alignées sur les normes internationales (par exemple, les principes directeurs des Nations unies, les lignes directrices de l'OCDE) pour que les entreprises prennent en compte les risques en matière de droits humains tout au long du cycle de vie de l'IA.

(ii) Les mécanismes de contrôle et d'évaluation du respect par les entreprises des normes en matière de droits humains[19] dans le contexte de l'IA, et les mécanismes permettant aux détenteurs de droits de demander réparation.

(iii) Des exemples de pratiques qui permettent aux entreprises d'assumer leur responsabilité en matière de respect des droits humains et d'engager les parties prenantes de manière significative dans le contexte de l'IA.[20]

(iv) Toute mesure, ligne directrice ou pratique sectorielle concernant les secteurs de gouvernance publique suivants[21] :

- *Application de la loi et sécurité publique*
- *Administration de la justice*
- *Soins de santé*
- *Éducation*
- *Services sociaux et protection sociale*
- *Immigration et contrôle des frontières*
- *Travail et emploi*
- *Logement et urbanisme*
- *Fiscalité*
- *Processus démocratiques*
- *Administration publique*

ANDORRA / *ANDORRE*

La Principauté d'Andorre a mis en œuvre des mesures, des directives et des pratiques spécifiques pour aborder les impacts potentiels sur les droits de l'homme des entreprises impliquées dans le cycle de vie des systèmes d'intelligence artificielle (IA) et fournir des solutions lorsque ces impacts se produisent.

En ce qui concerne le Code éthique sur l'IA, il met en évidence l'importance d'adopter une approche éthique et juridique dans le développement et l'utilisation de l'IA. Le Code éthique insiste sur la protection des droits fondamentaux, tels que la dignité, l'autonomie, l'égalité et la

depuis la conception d'un système d'intelligence artificielle jusqu'à sa mise hors service, quel que soit l'acteur qui y participe ».

[19] *Voir la section III de l'annexe à la Recommandation CM/Rec(2016)3 du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises.*

[20] *Voir par exemple l'article 67 (forum consultatif) du règlement (UE) 2024/1689 établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'IA de l'UE) concernant la création d'un forum consultatif.*

[21] *Pour plus de détails sur les secteurs de gouvernance publique énumérés, voir le document CDDH-IA(2024)06REV.*

non-discrimination, ainsi que sur la vie privée et la sécurité des personnes. Il souligne également la nécessité de réaliser des évaluations d'impact éthique et des droits de l'homme avant la mise en œuvre de systèmes d'IA, afin d'éviter d'éventuels préjudices pour les personnes concernées. Compte tenu des caractéristiques du pays, Andorre privilégie une réglementation spécifique de nature sectorielle dans les domaines stratégiques en ligne avec la Stratégie nationale de transformation numérique à l'horizon 2030. Toutefois, il convient de noter que l'Andorre est en processus d'association avec l'Union européenne qui comportera, une fois l'Accord d'Association en vigueur, des implications directes sur le cadre juridique de l'intelligence artificielle dans le pays.

Dans l'affirmative, merci de fournir des détails, notamment sur :

(i) Les cadres juridiques ou politiques en place, y compris les obligations spécifiques ou les lignes directrices alignées sur les normes internationales (par exemple, les principes directeurs des Nations unies, les lignes directrices de l'OCDE) pour que les entreprises prennent en compte les risques en matière de droits humains tout au long du cycle de vie de l'IA.

La Principauté d'Andorre a signé la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit. Le Gouvernement travaille actuellement, dans la mise en place des structures administratives et l'adoption de la législation pertinente en vue de permettre la ratification de ladite Convention. De plus, tel que susmentionné, le Gouvernement a approuvé le Code éthique sur l'IA, pour la régulation des relations entre l'IA et les droits de l'homme.

Le Code éthique de l'intelligence artificielle d'Andorre établit un cadre clair et détaillé, avec des lignes directrices pour garantir que l'IA soit développée et utilisée de manière éthique et responsable, en protégeant les droits de l'homme à toutes les étapes du cycle de vie des systèmes d'IA.

Le Code met l'accent sur l'importance d'une approche holistique et responsable qui favorise la confiance dans l'application et l'utilisation de l'IA, en mettant les personnes au centre du développement technologique. Parmi les mesures phares, on trouve :

1. Évaluations d'impact éthique et des droits de l'homme : Avant de déployer des systèmes d'IA, il est recommandé de réaliser des évaluations d'impact éthique et des droits de l'homme pour identifier et atténuer les risques potentiels.
2. Principes de conception légale et éthique : Le principe des droits de l'homme par la conception (HRbD) est promu, ce qui implique de considérer la protection des droits de l'homme dès la phase de conception de tout projet, initiative, produit ou service basé sur l'IA.
3. Transparence et explicabilité : Il est établi que les systèmes d'IA doivent être transparents et explicables, permettant aux utilisateurs de comprendre leur fonctionnement et la manière dont les décisions automatisées sont prises.
4. Supervision et contrôle humains : Une supervision et un contrôle humains sont garantis sur les processus des systèmes d'IA, assurant que la responsabilité finale incombe aux êtres humains.
5. Mécanismes de réclamation et de réparation : Des mécanismes efficaces et accessibles de réclamation, de recours et de réparation sont établis pour les personnes affectées ou menacées par les systèmes d'IA.

Ces mesures reflètent l'engagement d'Andorre en faveur de la protection des droits de l'homme dans le contexte de l'intelligence artificielle, s'alignant avec des cadres internationaux tels que la Recommandation sur l'éthique de l'intelligence artificielle de l'UNESCO et les directives de l'OCDE et de l'Union européenne.

Andorre, en ligne avec d'autres initiatives internationales et nationales similaires qui se produisent au niveau mondial, pour promouvoir l'IA de confiance, ainsi qu'avec les objectifs et axes stratégiques du Programme de Transformation Digitale (PdTDA) du pays, plaide en faveur des modèles et des écosystèmes numériques responsables, en misant sur l'innovation sans compromettre les droits et libertés fondamentaux des personnes garantis par la Constitution et la législation andorrane.

Le Code d'Éthique de l'Intelligence Artificielle d'Andorre cherche à soutenir, guider et orienter le secteur public, le secteur privé et les citoyens (parties prenantes et destinataires du Code), dans le chemin nécessaire vers la pleine réalisation et promotion de l'IA de confiance dans les différents domaines d'action concernés.

(i) Les mécanismes de contrôle et d'évaluation du respect par les entreprises des normes en matière de droits humains dans le contexte de l'IA, et les mécanismes permettant aux détenteurs de droits de demander réparation.

Le Gouvernement andorran a créé l'Agence d'Intelligence des Données (*Décret 327/2024, de 21 août 2024, du gouvernement des données et de création de l'Agence d'Intelligence des Données*), organisme spécifique et spécialisé dans le domaine pour répondre aux divers défis liés à l'interopérabilité, à la gouvernance des données et à l'intelligence artificielle en Andorre.

En effet, la gouvernance des données doit constituer l'un des piliers fondamentaux de l'administration numérique du Gouvernement, c'est pourquoi il est nécessaire d'établir un modèle de données propre, ainsi que de répondre aux différents défis liés à l'interopérabilité, à la gouvernance des données et à l'intelligence artificielle.

Sous l'égide de cette réglementation et avec les mêmes objectifs, le Gouvernement d'Andorre a créé son propre Bureau d'Intelligence des Données (*Décret 328/2024, de 21 août 2024, de création du Bureau d'Intelligence des Données de l'Administration Générale*), en tant que bureau d'impulsion de l'administration numérique pour faciliter, entre autres, le déploiement des bonnes pratiques concernant l'intelligence artificielle.

Le Bureau d'Intelligence des Données, en relation avec la matière de l'intelligence artificielle (IA) dans le cadre de l'Administration générale, exerce les fonctions suivantes :

a) Contribuer à la mise en œuvre, au suivi et à la supervision des systèmes d'IA et à la gouvernance de l'IA.
b) Contribuer à la promotion d'actions et de politiques visant à tirer parti des bénéfices sociaux et économiques des technologies d'IA.
c) Soutenir le développement, l'implantation et l'utilisation accélérée de systèmes et d'applications d'IA fiables apportant des bénéfices sociaux et économiques et contribuant à la compétitivité et à la croissance économique.
d) Contribuer à une approche stratégique, cohérente et efficace concernant les initiatives nationales et internationales en matière d'IA.
e) Développer des outils, des méthodologies et des indices de référence pour évaluer les capacités des modèles d'IA.

f) Superviser l'exécution et l'application des normes relatives aux modèles et systèmes d'IA à usage général, en particulier lorsque le modèle et le système sont développés par le même fournisseur.
g) Surveiller l'apparition de risques imprévus découlant de modèles d'IA à usage général, en particulier en répondant aux alertes du groupe d'experts scientifiques.
h) Enquêter sur d'éventuelles infractions aux normes relatives aux modèles et systèmes d'IA à usage général.
i) Soutenir l'application des normes relatives aux pratiques d'IA interdites et aux systèmes d'IA à haut risque.
j) Développer, soutenir et mettre en œuvre le code éthique de l'IA.
k) Toute autre fonction qui lui est confiée.

(ii) Des exemples de pratiques qui permettent aux entreprises d'assumer leur responsabilité en matière de respect des droits humains[22] et d'engager les parties prenantes de manière significative dans le contexte de l'IA.[23]

Le Code éthique sur l'IA établit des lignes directrices assorties d'un certain nombre de recommandations pour le secteur privé :

Objectif recommandé	**Description**
Fiabilité de l'IA	Veiller à ce que l'IA soit digne de confiance, solide et sûre, en adoptant les politiques, systèmes ou processus les plus appropriés à tout moment pour atteindre ces objectifs.
Respecter les valeurs et les principes éthiques	Dès la phase de conception, favoriser le développement et la mise en œuvre de systèmes d'IA qui respectent les principes éthiques, les valeurs et les droits de l'homme, ainsi que les réglementations et normes internationales pertinentes, en adoptant des mesures préventives, correctives et de responsabilisation tout au long du cycle de vie de ces systèmes.
Respecter les droits et les libertés des personnes	Centré sur les personnes, en particulier : respecter la dignité, l'autonomie, l'égalité, la non-discrimination, la vie privée et la sécurité des personnes concernées par les systèmes d'IA, parmi d'autres droits et libertés fondamentaux.
Afin de s'acquitter de leur responsabilité en matière de respect des droits de l'homme, les entreprises doivent mettre en place des politiques et des procédures adaptées à leur taille et à leur situation	Afin de s'acquitter de leur responsabilité en matière de respect des droits de l'homme, les entreprises doivent mettre en place des politiques et des procédures adaptées à leur taille et à leur situation. Il s'agit notamment des éléments suivants :

[22] Voir la section III de l'annexe à la Recommandation CM/Rec(2016)3 du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises.
[23] Voir par exemple l'article 67 (forum consultatif) du règlement (UE) 2024/1689 établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'IA de l'UE) concernant la création d'un forum consultatif.

	1) s'engager à assumer la responsabilité de respecter les droits de l'homme ; 2) des processus et une diligence raisonnable en matière de droits de l'homme afin d'identifier, de prévenir et d'atténuer les incidences sur les droits de l'homme et d'en rendre compte ; 3) des processus visant à remédier à toute incidence négative sur les droits de l'homme qu'elles ont causée ou à laquelle elles ont contribué.
Identifier et évaluer les impacts négatifs associés à l'IA	Identifier et évaluer les impacts négatifs réels ou potentiels associés aux projets, initiatives, produits et services de l'entreprise sur les droits et libertés fondamentaux des personnes, la sécurité et le développement durable.
Prévenir les impacts négatifs de l'IA	Arrêter, identifier et évaluer les impacts négatifs réels ou potentiels associés aux projets, initiatives, produits et services de l'entreprise sur les droits et libertés fondamentaux des personnes, la sécurité et le développement durable.
Mécanismes de diligence, de responsabilité et de transparence	Prévoir des mécanismes de diligence raisonnable, de responsabilité et de transparence lors de la conception, du développement et de l'utilisation de l'IA, en tenant compte des incidences susmentionnées et de leurs effets négatifs.
Mécanismes de réclamation et de recours	Mettre en place des mécanismes de plainte, de recours et de réparation efficaces et accessibles pour les personnes blésées ou menacées par les systèmes d'IA.
Mettre en place des systèmes de gestion des risques et de contrôle pour les systèmes d'IA	Mettre en place des systèmes de gestion des risques et de contrôle qui garantissent la sécurité, la fiabilité et la robustesse à long terme des systèmes d'IA.
Transparence, traçabilité et explicabilité des systèmes d'IA	Garantir la transparence, la traçabilité et l'explicabilité des systèmes d'IA, en fournissant des informations claires et accessibles sur les objectifs, les capacités, les limites, le fonctionnement et les sources de données de ces systèmes, ainsi que sur les rôles et les responsabilités assumés par les parties prenantes concernées.
Qualité des données	Garantir la qualité, l'intégrité, la diversité, la représentativité et la sécurité des données utilisées pour former, déployer et exploiter les systèmes d'IA, en évitant les biais, les discriminations, les stéréotypes et les

	préjugés injustifiés ou portant atteinte aux droits des personnes.
Formation et alphabétisation en matière d'IA	Favoriser l'acquisition de compétences numériques et d'une culture de l'intelligence artificielle, en particulier pour les salariés et assimilés, et dans l'ensemble des organes de direction et d'administration de l'entreprise.
Favoriser une culture de l'innovation responsable	D'une manière générale, favoriser une culture de l'innovation responsable qui profite à la fois aux entreprises et à la société, en collaborant et en coopérant avec les différents acteurs et secteurs concernés, y compris les autorités compétentes, la société civile, le monde universitaire et les utilisateurs finaux.
Participer à des consultations publiques et à des processus délibératifs sur la réglementation et la gouvernance de l'IA	Participer à des consultations publiques et à des processus délibératifs sur la réglementation et la gouvernance de l'IA et exprimer ses opinions et ses préoccupations. Soutenir les initiatives en faveur de l'innovation, de la compétitivité des entreprises, des personnes et de la planète.

Pour en savoir plus, voir le Code éthique sur l'IA sur le site (version anglaise): Codi etic english.pdf

(iii) Toute mesure, ligne directrice ou pratique sectorielle concernant les secteurs de gouvernance publique suivants[24]:

- Application de la loi et sécurité publique
- Administration de la justice
- Soins de santé
- Éducation
- Services sociaux et protection sociale
- Immigration et contrôle des frontières
- Travail et emploi
- Logement et urbanisme
- Fiscalité
- Processus démocratiques
- Administration publique

La Stratégie Nationale de Transformation Digitale d'Andorre considère les administrations publiques comme l'un des axes centraux du Programme de Transformation Digitale à travers l'optimisation de l'efficacité administrative par le biais des technologies de l'information et l'établissement de canaux de communication numérique avec les citoyens.

CYPRUS / *CHYPRE*

The Republic of Cyprus is in the process of implementing Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act).

[24] Pour plus de details sur les secteurs de gouvernance publique énumérés, voir le document CDDH-IA(2024)06REV.

The European Commission has signed the Council of Europe Framework Convention on Artificial Intelligence (AI) on behalf of the EU.

Contribution from The Deputy Ministry of Research, Innovation and Digital Policy (DMRID):

The Deputy Ministry of Research, Innovation and Digital Policy (DMRID) of the Republic of Cyprus has notified the European Commission of the national public authorities that will supervise and enforce compliance with the obligations under EU law to protect fundamental rights, in accordance with the Article 77 of Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act) as follows:

- Commissioner for Personal Data Protection
- Commissioner for Administration and the Protection of Human Rights (Ombudsman)
- Attorney-General of the Republic of Cyprus

The authorities included in this list will be granted additional powers under the Regulation to facilitate the exercise of their existing responsibilities to protect fundamental rights in cases where the use of artificial intelligence (AI) poses high risks to these rights. These powers will take effect from 2 August 2026.

In parallel, as part of the implementation of the European Artificial Intelligence Act (AI Act), Cyprus has recently designated the national competent authorities, which were to include at least one Notifying Authority and at least one Market Surveillance Authority.
Specifically, the following authorities have been designated:

- The Commissioner of Communications is appointed as the Notifying Authority and the Market Surveillance Authority, acting as the Single Point of Contact for the AI Act.
- The Commissioner for Personal Data Protection is also appointed as a Market Surveillance Authority for matters related to her areas of competence.

This governance structure reinforces Cyprus's commitment to safeguarding fundamental rights and promoting the responsible and ethical use of Artificial Intelligence."

- Education

Contribution from the Ministry of Education, Sport and Youth:

"Measures, Guidelines, or Practices to Address Human Rights Impacts of AI

The Ministry of Education, Sport and Youth has undertaken several initiatives to ensure the responsible integration of AI in education while safeguarding human rights. These measures include:

1. Compliance with GDPR:
    - The Ministry strictly adheres to the General Data Protection Regulation (GDPR), ensuring that all AI tools used in education comply with robust data protection and privacy standards for students and educators.
2. Establishment of a Monitoring Group:
    - A dedicated working group within the Ministry monitors and assesses the compliance of AI systems with human rights standards. This group is responsible for identifying potential risks and ensuring transparency and accountability in AI use.
3. Development of a Comprehensive AI Framework:
    - The Ministry is in the process of developing a comprehensive framework for AI integration into the education system. This framework will provide clear guidelines on the ethical use of AI, focusing on protecting human rights, ensuring equitable access, and fostering inclusion.

4. Support for Educators:
    - Educators across Cyprus use AI-enabled tools to enhance lesson preparation and create innovative educational materials. These tools support personalized learning and resource accessibility while being subject to compliance checks under the aforementioned framework.

Sector-Specific Measures

The Ministry has implemented various actions and strategies to ensure the ethical integration of AI in education:

1. Promotion of AI Policies in Education:
    - Adopting and adapting frameworks, practices, and recommendations from international and European contexts.
    - Prioritizing educator and staff training on AI integration.
    - Developing practical guidelines to assist educators in using AI tools effectively and ethically.
2. Unified AI Integration Approach:
    - Showcasing the potential benefits of AI tools in improving educational processes.
    - Addressing limitations, challenges, and vulnerabilities of AI, including ethical considerations and data privacy concerns.
3. Implementation of Training Programs:
    - Regular seminars, workshops, and training programs since 2019 for educators and Ministry staff.
    - Responding to specific requests from schools and educators for AI-related training.
    - Participation in national, European, and international AI-related working groups to align with global best practices.
4. Mapping of AI Integration Initiatives:
    - A comprehensive map of actions highlights the integration of AI into curricula and informal education.
    - Supported by a tool proposed by the Pedagogical Institute, this effort enables a structured approach to mapping AI initiatives.
5. Roadmap for Immediate Actions:
    - As outlined in the approved AI Utilization Roadmap of the Ministry, immediate actions include the establishment of an Advisory Committee on AI in Education. The Pedagogical Institute will lead this initiative, with formal invitations to expert consultants and the official formation is expected by January 2025.

Examples of AI Tools and Their Usage in Education

The Ministry has identified several aspects of AI usage in education:

1. Current Usage:
    - Educators use AI tools to assist with lesson planning, creating exercise sheets, and generating educational materials. These tools support personalized learning and streamline administrative tasks.
2. Concerns Regarding Student Usage:

- Educators have raised concerns about students' reliance on AI tools for completing assignments outside school settings. The lack of parental knowledge about these tools underscores the need for awareness and guidance.

3. Addressing Ethical Challenges:
   - The Ministry recognizes the importance of addressing challenges related to ethical AI use. Plans are underway to raise awareness among parents, educators, and students about responsible AI usage.
4. Lack of Formal Assessment:
   - While no formal assessment has been conducted to measure the benefits or challenges of AI usage, the planned Advisory Committee is expected to guide future evaluations."

- Social Services and Welfare

Contribution from the Deputy Ministry of Social Welfare:

Artificial Intelligence and persons with disabilities

Artificial Intelligence (AI) has the potential to greatly improve the lives of persons with disabilities, but also it has a lot of risks. These risks can be significant, and Artificial Intelligence (AI) should be ensured that is developed safely with accessibility and inclusion in mind. As about protecting the accessibility, the "Accessibility of Products and Services Law of 2024" was approved by our Parliament and will support the development of the universally accepted accessibility standards to ensure that digital products and services are accessible and usable by all people, including persons with disabilities.

As about ensuring the protection of personal data of persons with disabilities which are maintained in public databases, access to all electronic systems is granted only to authorized users who can enter the system only with the use of a personal password. In addition, in all public services, there are personal data officers who are liaisons with the Office of the Commissioner for Personal Data Protection and guide the staff regarding the procedures for the safeguarding of personal data. As about the upgrading of the digital skills of people with disabilities, an action has been included in the Revised National Disability Strategy and Disability Action Plan 2024-2028, that will be conducted by the Deputy Ministry of Research, Innovation and Digital Policy. The action concerns the assessment of the specific needs of people with disabilities and the design of a series of trainings in collaboration with the Cyprus Productivity Centre and various social partners.

Beyond the above, persons with disabilities must be involved in discussions to ensure the AI does not lead to discrimination. For this reason, consultation with the Cyprus Confederation of the Organisations of the Disabled is regulated by a special law (the 2006 Law on the Consultation Procedure of State and Other Services in Matters Concerning Persons with Disabilities). Not only the Confederation but all representative organisations of persons with disabilities are informed and actively involved in the decision-making process regarding the formulation and adoption of policies, measures and actions.

- Labour and Employment

Contribution from the Ministry of Labour and Social Insurance

With reference to the provisions of the Safety and Health at Work legislation (although the AI is not specifically mentioned), the employers are obliged to get their workers, familiarized with the use of AI in the workplace and its relevance regarding workers' role and duties, making sure that they understand the ethical implications of AI. Furthermore, the deployment of AI in the workplace poses new and emerging risks that might compromise occupational safety and health; therefore, the risk assessment and implementation of preventive and protective measures is of critical importance. Continuous learning,

upskilling and reskilling for workers, as well as provision of specific and clear instructions must be ensured, to eliminate human oversight and accountability in high-risk environments.

CZECHIA / *TCHÉQUIE*

The Czech Republic will address these issues by gradually implementing the EU's AI Act. However, two national AI policies have been adopted already.

In 2019 the Government approved first National Artificial Intelligence Strategy of the Czech Republic (available in English here: https://mpo.gov.cz/assets/cz/rozcestnik/pro-media/tiskove-zpravy/2019/6/NAIS_eng_korektura_06-19_web.pdf).

In 2024 the Government approved National Strategy for Artificial Intelligence of the Czech Republic 2030 (available in Czech here: https://mpo.gov.cz/assets/cz/rozcestnik/pro-media/tiskove-zpravy/2024/8/AI_strategie_1.pdf; press release in English available here: https://mpo.gov.cz/en/guidepost/for-the-media/press-releases/czechia-as-a-technological-leader--government-approved-the-national-strategy-for-artificial-intelligence-of-the-czech-republic-2030--282278).

Both strategies warn that in addition to the benefits of AI, there are potential risks as well. They were also prepared in close cooperation with the representatives of the private sector.

The 2019 Strategy did not specifically mention human rights but had one chapter dedicated to legal and societal aspects of AI, ethical rules, consumer protection and security issues. The chapter briefly described short, medium and long-term objectives and appropriate tools how to achieve them. It calls for the revision of legislation with an emphasis on preventing discrimination, protecting rights and privacy due to AI. It also mentions that the OECD, UN and other organisations have activities in this sector, provide recommendations etc. albeit without giving any details in this regard.

The 2024 Strategy is more detailed. It states that risks associated with the human rights, ethical and legal aspects of its development and use are increasingly being discussed and require appropriate measures at the national and international level. In this regard, the 2024 Strategy refers to specific documents prepared by international organizations such as UN, OECD, ITU. In addition, it set goals and potential measures. It also calls for the human-centred approach which requires protection of individual rights and consideration of individual interests across decision-making processes and the AI life cycle. Related to this are the concepts of human rights and ethics. The 2024 Strategy provides vision in key areas and the role of private actors. It focuses on seven priorities including ethical and legal aspects of AI. This part of the strategy states that establishing a functional and predictable legal framework and ensuring compliance with the constitutional order and international human rights obligations is a prerequisite for the current use of AI in the private and public sectors and its future technological development. The underlying principle is to ensure that AI technologies are consistent with democratic values and the fundamental rights and freedoms of individuals, using tools appropriate to the challenges in this area. The AI systems developed, operated and used in the Czech Republic must respect the rights and freedoms of individuals and be based on applicable legislation, ethical principles, respect for privacy and data protection and the latest knowledge of good practice in the field of cyber security.

As to other activities, there is also a proposal for the project called “Activities of the Ethics Committee for the Assessment of Issues Related to the Operation of Automated and Autonomous Vehicles in the Czech Republic”. The aim of the project is to continue the activities of the Ethics Committee for the Assessment of Issues Related to the Operation of Automated and Autonomous Vehicles in the Czech Republic from 1 April 2020 to 31 December 2028. Further details are unknown at this moment.

In addition to your questions, I am sending extra information regarding the use of AI systems in different branches of the Government:

- **Immigration and Border Control:** In September 2024, the Government approved amendments to the Police Act and other laws. According to this draft legislation, the Police will be allowed to use security measures with an isolated AI system at the Václav Havel Airport in Prague and subsequently other international airports in the Czech Republic. Basically, it will enable remote real time identification in a database for a specifically defined groups of individuals (for example terror suspects, deported foreigners, etc). The system will not be able to recognise any other individuals outside these specific groups. Permission to enter a person into the database must be approved by the court. The draft legislation refers to the ECtHR’s judgment in case of *Glukhin v. Russia*, no. 11519/20, judgment of 4 July 2023. The amendment must pass the legislative process in the Parliament. However, the pilot mode has been tested already using the NEC NeoFace Watch a NeoFace Archiver technology.

- **Law Enforcement and Public Safety:** The Ministry of the Interior is working on a tool to combat voice deepfakes. The project aims to develop a system combining voice biometrics and artificial voice identification. The project responds to current threat related to voice modification and synthesis systems. It will contribute to detecting attempts to commit crime.

- **Social Services and Welfare:** The Ministry of Labour and Social Affairs (MoLSA) uses AI in production mode in the area of social assistance. The AI system extracts information from handwritten parental allowance applications and transcribes them into the agenda system. No other scenarios are used in this mode. However, the MoLSA is planning to use AI in other areas to save time and costs. In 2024 the MoLSA launched a voicebot/chatbot for client services. It answers questions outside of working hours or if none of the employees is available. It can also advise on state social assistance benefits or topics related to employment. A new version will be able to look into the person’s file and give basic information about the status of his or her application.

- **Housing and Urban Planning:** In one region, fifteen municipalities launched a project using AI. It enables to order cars or minibuses for people from small villages that leave on call. This way regular and almost empty buses do not have to run. The AI system interacts with a calling person, plans the journey according to person requirements and chooses the best route, all in real time. The AI system can also handle the control of regional subsidies for municipalities.

- **Administration of Justice:** The Ministry of Justice uses the BEEY image and voice recognition technology, which is also available to courts. It automatically converts audio and video to text. It also includes tools for quick editing of transcribed text. The technology is also used by the Parliament, Police, Czech National Bank etc.

DENMARK / *DANEMARK*

The Danish Data Protection Agency (DPA) has published guidelines on the use of AI in the public sector. The guidelines address data protection considerations for developing and deploying AI solutions in the public sector. The guidelines highlight the importance of safeguarding the fundamental rights of data subjects. Included in the guidelines are considerations on legal basis, the right to be informed and Data Protection Impact Assessments (DPIAs). The introductory chapter of the guidelines refers to the definition of 'AI system' from the OECD's 'Recommendation of the Council on Artificial Intelligence'.

Additionally, the Danish DPA has published a template for carrying out DPIAs in accordance with the GDPR when using AI solutions. The template requires that relevant risks – as well as the likelihood and severity of the risks – to the rights and freedoms of data subjects have been assessed, and all relevant mitigating measures are described.

FRANCE

Pas de réponse.

GEORGIA / *GÉORGIE*

(i) The legal or policy frameworks in place, including specific obligations or guidelines aligned with international standards (e.g., UN Guiding Principles, OECD Guidelines) for businesses to address human rights risks across the AI lifecycle.

Georgia has not yet implemented any specific measures, guidelines, or practices which aim to address potential impacts on human rights by businesses involved in the artificial intelligence systems lifecycle, and to provide remedies when such impacts occur, but through Digital Governance Agency, Georgia actively contributes to the work of the Council of Europe Committee on Artificial Intelligence (CAI). The country has signed the Council of Europe Framework Convention on Artificial Intelligence on 5 September 2024, demonstrating its commitment to integrating AI governance into its legislative framework. As of existing data protection laws, there are no specific provisions regulating AI, but by general clauses AI is also covered by some of them. For instance, the Law of Georgia "On Personal Data Protection" ensures safeguards against potential human rights violations in general, including those associated with the use of AI technologies in personal data processing. Data protection impact assessments are mandatory for businesses deploying high-risk systems, which also could include AI systems as well.

An important regulatory instrument in this context is the Order of President of the National Bank of Georgia "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence and Machine Learning Models" (Order No. 151/04; 17 August 2020). This regulation aims to establish a robust risk management framework for data-driven statistical, artificial intelligence, and machine learning models, ensuring the effective mitigation of associated risks. It outlines the processes for developing and utilizing such models and specifies their key components for entities under the supervision of the National Bank of Georgia, including commercial banks, micro banks, non-bank depository institutions, microfinance organizations, credit information bureaus, and loan-granting legal entities.

Additionally, Georgia is currently in the early stages of developing a comprehensive artificial intelligence policy framework and associated reforms. While these efforts are underway, the Georgia's Innovation and Technology Agency (GITA) has been particularly proactive within its mandate. GITA is leading several initiatives aimed at fostering the development and integration of AI technologies across various sectors. Specifically, the Agency is about to start developing Georgia's first National AI Strategy and its corresponding Action Plan. This policy document will set the national vision for AI and identify strategic interventions to guide AI development in various sectors, ensuring that ethical and responsible AI principles are integrated.

Moreover, plans are underway to set up Georgia's first AI Center of Excellence at the Kutaisi Techhub. The Center's objectives include: Developing a core Georgian AI model to aid local businesses, government and academia; [Business AI & Government AI] Enhancing AI solutions through robust computing infrastructure; [Computing Resources] Providing access to high-performance computing resources to accelerate AI applications; [Community Engagement] Facilitating interaction within the AI and technology communities to foster innovation; [Academic Support] Promoting academic research and teaching by improving access to resources. It is also planned that as part of the AI Centre of Excellence initiative, a regulatory sandbox will be created. This innovative platform will allow businesses to test AI solutions and applications within a controlled environment, specifically designed to include mechanisms for assessing the impact on human rights. This setup aims to balance technological innovation with ethical accountability, offering a transparent, accountable framework for the ethical deployment of AI in the future.

(ii) Mechanisms for monitoring and assessing business compliance with human rights standards in the context of AI, and mechanisms through which rights holders may seek remedies.

As of now, Personal Data Protection Service monitors the lawfulness of personal data processing including in the application of AI technologies. Meanwhile Public Defender (Ombudsman) of Georgia is a constitutional institution, which supervises the protection of human rights and freedoms within its jurisdiction on the territory of Georgia. It identifies the violations of human rights and contributes to the restoration of the violated rights and freedoms. There are several more authorities having mandate over supervising the protection of human rights from different perspective (e.g. Energy Ombudsman, Ombudsman of the National Bank of Georgia, etc.). The determination of whether to establish a new competent authority to oversee the creation of controlled environments for the development, experimentation, and testing of artificial intelligence systems, or to amend the mandate of an existing authority, shall be made during the ratification process of the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law.

(iii) Examples of practices that enable corporate responsibility to respect human rights2 and meaningful stakeholder engagement in the context of AI (for e.g. advisory forums or regular meetings).

Although Georgia does not yet have specific regulations exclusively addressing AI, the country’s personal data protection legislation obliges all corporations in the private sector to respect human rights when processing personal data. This serves as a foundational safeguard for the human rights in the context of AI.

Regarding stakeholder engagement, under Georgian national legislation, every policy document must go through a **public consultation** phase. Furthermore, public consultations are often held before the Parliament adopts new regulations, ensuring transparency and inclusion. Additionally, noteworthy, that the upcoming Digital Governance Strategy of Georgia (2025–2030) includes a plan to establish a Public-Private Partnership platform in the digital governance domain. This platform will act as a forum for discussions between business and government representatives on various topics, including AI-related issues.

(iv) Any sector specific measures, guidelines, or practices concerning the following public governance sectors:

No sector specific measures, guidelines or practices exist concerning the above-mentioned public governance sectors.

GREECE / *GRÈCE*

a. The following were reported by the Supreme Court (“Areios Pagos”) on the use of AI in the **administration of justice**:

“One of the artificial intelligence applications, which is developed and will be used by the Greek criminal courts, is that of the anonymization of court decisions. This application is included and is expected to be in use, soon, through the Integrated Judicial Case Management System for Civil and Criminal Cases (OSDDY-PP) with full respect for personal data, based on the provisions of Law 4624/2019 [Government Gazette A' 137/29-8-2019), "Hellenic Data Protection Authority, measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and transposition into national law of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 and other provisions.".

In Greece, as far as the artificial intelligence applications is concerned, Law 4961/2022 (Government Gazette A' 146/27-07-2022 on "Emerging information and communication technologies, strengthening digital governance and other provisions”) was published and set in force, with the aim to establish the adequate regulatory framework for the legitimate and secure exploitation of the potential of AI by public and private sector, as well as to strengthen the resilience of the public administration against cyber threats.

As emphasized in Article 1 of the aforementioned Law, its provisions do not affect, in any way, the rights and obligations deriving from EU and national law on the protection of personal data and private life and in particular, from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (L 119) (General Data Protection Regulation - GDPR) and from Law 4624/2019 (A' 137), within the framework of the processing of personal data that takes place when using artificial intelligence systems.

Within the context of the provisions and requirements of Law 4961/2022 (Government Gazette A' 146/27-07-2022), the Ministry of Justice of Greece has established a Steering Committee, chaired by a Vice-President of the Council of State, with the objective of examining the impact of the

introduction of artificial intelligence in the judicial system (Permanent Scientific Committee for Artificial Intelligence). The following issues are discussed:
- The actions of the Ministry of Justice regarding the use of artificial intelligence applications.
- Artificial intelligence applications at the Athens Court of First Instance for the Electronic Provision of Court Decisions to lawyers.
- The pilot system for creating document summaries and deleting / omitting personal data.
- Digital Assistants to support the drafting of court documents, including court decisions, to seek, based on Greek Law, information (in a R&A form) about the judicial system and to provide instructions to citizens and lawyers concerning electronic and non-electronic services of the Greek Justice.

Finally, the competent departments of the Ministry of Justice are examining, on a pilot basis, the possibility of using artificial intelligence applications for interpreting and translating documents, as well as for converting audio into text, aiming at facilitating the drafting of court hearing minutes."
The afore-mentioned Steering Committee has proceeded with the translation into Greek of CEPEJ' Ethical Charter(https://ministryofjustice.gr/wp-content/uploads/2020/07/CEPEJ_Chart_GR.pdf). It has also proposed (November 2024) the adoption of Guidelines for the anonymization of judicial decisions.

b. The aforementioned **Law 4961/2022** was an initial attempt to establish a **framework for the responsible use of artificial intelligence**. Among its key provisions is the obligation to conduct an algorithmic impact assessment before using AI systems by public sector entities, aimed at assessing risks to citizens' rights and freedoms. Specifically, Article 4 of Law 4961/2022 provides for the use of AI systems for decision-making or decision-support processes or the issuance of acts that affect the rights of a natural or legal person, only if this use is explicitly provided for in a special legal provision that includes appropriate safeguards for the protection of these rights. Additionally, according to Article 6 of the same law, the public sector is required to adhere to principles of transparency when using AI systems, while Article 7 imposes on the contractors of the systems the obligation to provide relevant information to public entities. Furthermore, Article 8 provides that information about AI systems, as well as algorithmic impact assessments conducted by public entities, must be recorded in a special registry, ensuring transparency and accountability.

At the same time, businesses are required to inform employees or prospective employees about the use of AI systems that affect employment decisions (regarding working conditions, selection, hiring, or evaluation), while medium and large companies are required to adopt ethical data use policies, which include measures to protect human rights when using artificial intelligence.
Any private sector business that uses an artificial intelligence system which affects any decision-making process related to employees or job candidates, and impacts their working conditions, selection, hiring, or evaluation, must, before the system is first used, provide adequate and clear information to each employee or job candidate. This information must include at least the parameters upon which the decision-making is based, subject to cases that require prior information and consultation. Additionally, the business must ensure the adherence to the principle of equal treatment and the fight against discrimination in employment and work on grounds of sex, race, color, national or ethnic origin, genealogical descent, religious or other beliefs, disability or chronic illness, age, family or social status, sexual orientation, gender identity, or gender characteristics. (article 9)

Public entities (article 8) and private businesses (article 10) that use AI systems within the framework of consumer profiling or within the framework of evaluating all types of employees or individuals working with the business (article 10) using AI systems must keep a register of AI

systems they use, containing all necessary information concerning their design, deployment, use, impacts etc. Businesses must establish and maintain a data ethics policy, which includes information regarding the measures, actions, and procedures it applies on data ethics issues when using artificial intelligence systems (article 11).

c. It is further noted that Greece, as a Member State of the European Union, is bound by **Regulation (EU) 2024/1689 (AI Act) and all AI-relevant EU legislation**. This includes, inter alia, the Digital Services Act or Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work, whose Chapter III ("algorithmic management") provides for limitations concerning automated monitoring systems or automated decision-making systems, the obligation of transparency with regard to them, human oversight, etc. with respect to persons performing platform work.
All provisions of Law 4961/2022 above concerning AI are currently under review by a special Working Group established at the Ministry of Digital Governance, to fully align with the provisions of the Artificial Intelligence Act (EU Regulation 2024/1689).

d. The Ministry of Digital Governance is in constant consultation with involved Ministries, Authorities, public and private entities, the academic and research community, as well as representatives of civil society, in shaping the governance framework for AI in Greece and the relevant legal framework. The creation of a more permanent **structure for consultation with stakeholders is being considered**. This structure may be developed within the **AI Observatory**, which has already been legislatively provided for and will soon be operational within the Ministry of Digital Governance. Its main mission will be to collect data on AI development in Greece, compile reports on AI-related activities, and interact with stakeholders in the AI ecosystem.

e. In the field of **labour**:
Three actions related to the use of AI systems in work/employment are highlighted by the Ministry of Labour and Social Insurance:

1) European Technical Support Instrument (TSI 2024)
A multi-country request was jointly submitted by Belgium, Greece, and Spain to the European Commission (DG REFORM) under the 2024 call for the European Technical Support Instrument (TSI 2024). The request was selected for funding and is currently being implemented in Greece (Directorate for the Fight Against Poverty, General Secretariat for Social Solidarity and Fight Against Poverty, Ministry of Social Cohesion and Family) and Belgium (Federal Public Service Social Security).
The approved project, titled "Strengthening Social Protection Capacity and Enhancing the Labour Market Integration of Minimum Income Scheme (MIS) Beneficiaries through the Application of Artificial Intelligence (AI) to Labour Market Supply and Demand Matching," aims to strengthen the capacity of national authorities to develop AI-driven digital solutions that support the labour market integration of MIS beneficiaries. Such tools can be used to guide MIS beneficiaries in their job search, helping them to shorten their job search duration and leading to more sustainable and better-quality career paths and social inclusion. In this vein, the Project will explore opportunities to use Artificial Intelligence (AI) technologies to increase the performance of such digital solutions while minimising the associated risks, and addressing the need for inclusive, sustainable, citizen-centric AI development, not only to transform the economy but also to address societal challenges like gender inequalities and the digital divide.
Among the outputs of the project are:
• Information collection from stakeholders
• Identification of promising data for digital solutions matching GMI beneficiaries with labour demand

• Data analysis on GMI beneficiaries and employers
• Learning events of international good practices
• Recommendations on data to be used for digital solutions matching GMI beneficiaries with labour demand
• Study on the design of an algorithm that maximizes the matching of supply and demand in the labour market for GMI beneficiaries and legal basis analysis for making relevant data available for digital solutions.

2) Technical Assistance Project - Evidence-Based Jobseeker Profiling and Feedback Mechanisms

The World Bank has carried out a study for the Greek Public Employment Service (DYPA) to develop an evidence-based statistical profiling tool that will assist job counselors in supporting jobseekers. This study is part of a wider EU-funded project aimed to support the implementation of a national skills framework for learning pathways. Profiling models are used by public employment agencies to estimate how far jobseekers are from the labour market. With this information, agencies can better allocate resources and determine the level of support different jobseekers should receive.
The tool aims to help DYPA optimize the allocation of job counselors' time as well as the provision of other services, by identifying which jobseekers should be prioritized for such services.
The profiling models presented in final report utilize machine learning (ML) techniques which are particularly well suited to statistical profiling. In the experiments, rich administrative datasets have been applied to ML frameworks to predict unemployment duration based on various factors, such as demographic characteristics, previous employment history, and labour market conditions. The report presents several ML models which test how accurately different measures of unemployment duration can be predicted. The performance of these models was assessed in evaluation pilots, using statistical accuracy measures and in terms of operational usefulness.

3) Participation of MEKY in the Expert Group on AI in the Labour Market (DELSA-OECD)

The purpose of the Group is to guide governments and stakeholders in ensuring the human-centered, responsible, and trustworthy use of AI within the labour market. Specifically, it seeks to:
Promote Benefits: Leverage AI to create employment opportunities, improve job quality, enhance worker productivity, and address labour market challenges, such as skills mismatches and inclusion of underrepresented groups.
Mitigate Risks: Prevent and minimize potential ethical, legal, and social risks associated with AI, including bias, discrimination, loss of worker autonomy, and mental and physical health risks.
Encourage Social Dialogue: Facilitate collaboration between employers, workers, and other stakeholders to adapt to AI-driven changes while ensuring compliance with labour standards.
Support Policy Development: Provide actionable principles and recommendations for governments to design policies that promote fairness, inclusiveness, and transparency in AI use within labor markets.

The outcome of the Group will be the OECD Recommendation on Artificial Intelligence in the Labour Market. Its aim is set to be finalized and adopted in 2025, reflecting feedback from stakeholders and ensuring alignment with international standards and frameworks on AI.

f. The following two documents are attached for further reference:
(i) Input on the Questionnaire by the Greek National Commission for Human Rights ; and
(ii) The recent policy document by the High-Level Advisory Committee on Artificial Intelligence (advisory body to the Prime Minister), “A Blueprint for Greece’s AI Transformation” (a summary of this document is to be found in document (i) above).

The National Strategy for Artificial Intelligence focuses on the overall social, economic, and international upgrading of the country, emphasizing vital sectors. In **education**, it promotes the integration of artificial intelligence into the educational system from the primary level and the implementation of retraining and upskilling programs for all citizens. At the same time, it supports the development of personalized educational material, with particular care for students from underprivileged families or with learning difficulties, while enhancing citizens' familiarity with the opportunities offered by artificial intelligence.
In the **health sector**, the strategy prioritizes the improvement of the National Health System, focusing on quality and personalized care, effective management of chronic and rare diseases, and ensuring patients' rights. Greece has already undertaken initiatives, such as the publication of the European Commission's Opinion on Bioethics and Technologies (EECB), which focuses on the impact of artificial intelligence on healthcare. This document highlights ethical issues related to the use of technology, proposing measures to maintain the quality and ethics of health services. It also emphasizes the need for continuous evaluation of applications by experts, and hearings of scientists and stakeholders have already been organized to enhance dialogue.
The strategy also includes actions to reduce the **ecological footprint** of technological development, enhance **cultural heritage** through digital means, and utilize artificial intelligence for personalized cultural experiences. It proposes improving the efficiency of public services by developing **smart infrastructures** and services that better serve citizens, and developing Greece as a global destination for investments in artificial intelligence and new technologies, through the creation of ecosystems that will enhance the country's productivity and prosperity.

ITALY / *ITALIE*

Yes, Italy is actively developing a comprehensive legal framework to regulate artificial intelligence (AI), emphasizing the protection of human rights throughout the AI lifecycle.

The Italian draft law on AI, approved by the Italian Council of Ministers in April 2024, aims to promote a fair, transparent, and responsible use of AI, following a human-centered approach, and to monitor potential economic and social risks, as well as risks to fundamental rights.

As for the legal and policy frameworks, the draft law aligns with international standards, including the European Union's proposed AI Act, the UN Guiding Principles on Business and Human Rights, and the OECD Guidelines on AI, emphasizing the need for AI systems to be safe, reliable, transparent, and respectful of human dignity and fundamental rights.

Specific obligations for businesses include ensuring that AI applications comply with existing regulations, promoting transparency in AI operations, and implementing measures to prevent discrimination and bias. The law also mandates that employers inform employees about the use of AI in the workplace, ensuring that AI applications do not violate human dignity or infringe on personal data confidentiality

As for mechanisms for monitoring and assessing business compliance with human rights standards in the context of AI, and mechanisms through which rights holders may seek remedies, The draft law proposes the establishment of a national supervisory authority responsible for overseeing AI applications and ensuring compliance with human rights standards. This authority would have the power to conduct audits, impose sanctions, and require corrective actions from businesses that fail to adhere to the regulations. Additionally, the law outlines mechanisms through which individuals can seek remedies if their rights are violated by AI systems, including

the right to access information about AI-driven decisions affecting them and the ability to challenge such decisions through administrative and judicial processes.

With regard to corporate responsibility and stakeholder engagement, the draft law encourages businesses to adopt codes of conduct and best practices that promote ethical AI use. Regular consultations and public forums are also recommended to facilitate meaningful stakeholder engagement, ensuring that diverse perspectives are considered in the development and implementation of AI systems.

As for sector specific measures, the Italian draft law on AI addresses a variety of sectors:

- **Healthcare:** AI applications in healthcare must prioritize patient safety, data privacy, and informed consent. The law mandates rigorous testing and validation of AI systems used in diagnosis and treatment, ensuring they meet established medical standards.

- **Education:** In the educational sector, the law emphasizes the importance of transparency and fairness in AI-driven tools used for student assessment and personalized learning. It requires that such tools be designed to prevent bias and support inclusive education.

- **Public Administration:** The law outlines guidelines for developing AI applications within public administration, ensuring compliance with national and European regulations, consistency with national strategies, and the development of training initiatives for staff.

LATVIA / *LETTONIE*

As to the measures that have already been implemented in relation to AI and human rights, the Government notes that two new provisions of the *Criminal Law* entered into force on 22 May 2024 and 22 October 2024, respectively. These provisions criminalise the use of deep-fake technology to influence the election process, as well as in the process of appointment or approval of a State official in the Parliament of the Republic of Latvia. The relevant provisions read as follows:

> "**Article 90^1 Influencing the election process through the use of deep-fake technology**
>
> For the preparation or dissemination of deliberately false discrediting information about a political organisation (party) or an association of political organisations (parties) or a candidate for the Member of the Parliament of the Republic of Latvia, a municipal council, or a Member of the European Parliament, using deep-fake technology, if committed during the pre-election campaigning period or on election day, -
>
> the applicable punishment is the deprivation of liberty for a period up to five years or temporary deprivation of liberty or probationary supervision, or community service.
>
> **Article 90^2 Influencing the process of election, appointment or approval of a State official in the Parliament through the use of deep-fake technology**
>
> For the preparation or dissemination of deliberately false discrediting information, using deep-fake technology, regarding a candidate to the office of a State official who is elected, appointed or approved by the Parliament, if it is committed during the process of election, appointment or approval of a State official as prescribed by law, -

the applicable punishment is the deprivation of liberty for a period up to five years or temporary deprivation of liberty or probationary supervision, or community service."

Furthermore, on 7 November 2024, amendments to the *Pre-election Campaign Law* entered into force, supplementing the *Law* with two new provisions regulating the use of AI systems in pre-election campaigning. The relevant provisions read as follows:

"**Article 3[1] Use of artificial intelligence systems in pre-election campaigning**

If, during the pre-election campaigning period, a representation of a person or an event that does not correspond to reality (image, audio, or video content) created by an artificial intelligence system is used in a paid pre-election campaigning or campaigning material, this shall be indicated clearly and unambiguously.

Article 31[1] Decision prohibiting the further distribution (placement) of pre-election campaigning material generated by an artificial intelligence system

(1) In the event of establishing a violation of the procedure for the use of an artificial intelligence system referred to in Article 3[1] of this *Law*, the Head of the Corruption Prevention and Combating Bureau shall adopt a decision on prohibition of further distribution (placement) of the relevant pre-election campaigning material created by an artificial intelligence system.

(2) In order to adopt the decision referred to in paragraph 1 of this Article, the Corruption Prevention and Combating Bureau shall obtain the opinion of an expert or other specialist in the field, assess the expediency of the decision, the feasibility of its implementation, as well as the proportionality of the decision.

(3) The Corruption Prevention and Combating Bureau shall publish information on the adoption, revocation or amendment of the decision referred to in paragraph 1 of this Article on its website without delay.
(4) The decision referred to in paragraph 1 of this Article may be appealed before the Administrative District Court. Submitting an application with the court shall not suspend the operation of the decision. The court shall review the decision in accordance with the procedure laid down in Article 29, paragraph 4, of this *Law*."

Turning to the legal framework and other measures that are currently planned in the field of AI and human rights in Latvia, the Ministry of Smart Administration and Regional Development has drafted a report "*On the Implementation of the Requirements of the Artificial Intelligence Act*" ('Report').[25] The Report has been prepared to ensure the implementation of the requirements of the *Artificial Intelligence Act* (*Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024*) in Latvia. The Report describes the current situation in Latvia in the field of AI, the requirements of the *Artificial Intelligence Act*, and defines the actions to be taken by public administration to ensure the implementation of the *Artificial Intelligence Act* at the domestic level (the authorities responsible for the implementation of the *Artificial Intelligence Act* and the respective deadlines for its implementation). The Report also identifies the necessary amendments to the domestic legal framework, the necessary resources for the implementation of

[25] Available in Latvian at: https://tapportals.mk.gov.lv/attachments/legal_acts/document_versions/a1e647e8-80e7-435b-aeef-c80e19dbcc51/download.

the *Artificial Intelligence Act*, as well as the implementation of the rules on penalties in the national legal system, which is required by the *Artificial Intelligence Act*.

Regarding the requirements and obligations of national public authorities or bodies, which would supervise or enforce the respect of obligations under EU law protecting fundamental rights, including the right to non-discrimination, in respect to the use of AI systems (Article 77 of the *Artificial Intelligence Act*), the Report currently provides that in Latvia the protection of fundamental rights will be ensured by the Ombudsperson. The Report envisages the necessary amendments to the domestic laws and regulations to designate the Ombudsperson as the responsible authority for the protection of fundamental rights and its respective functions and tasks, as well as the modalities of cooperation with the market surveillance authorities in the field of the protection of fundamental rights (Article 77, paragraph 1, of the *Artificial Intelligence Act*). However, it should be noted that the Report is currently only being discussed between the competent ministries, institutions, and other stakeholders and has not been yet adopted.

Furthermore, a draft law – *Artificial Intelligence Development Law* – has been submitted before the Parliament for consideration.[26] The aim of the draft law is to create an ecosystem of AI technologies and determine the legal framework for cooperation between the public and private sectors, and universities. Additionally, with the above draft law, the authorities plan to establish the National Artificial Intelligence Centre, which will ensure that AI systems are used ethically, responsibly, and safely with due respect for fundamental human rights.

LIECHTENSTEIN

No.

LITHUANIA / *LITHUANIE*

(i) The legal or policy frameworks in place, including specific obligations or guidelines aligned with international standards (e.g., UN Guiding Principles, OECD Guidelines) for businesses to address human rights risks across the AI lifecycle.

Additionally, implementing the Article 77(2) of EU AI Act, Lithuania has published the list of national public authorities or bodies, which protect fundamental rights under Union law, using high-risk AI systems referred to in Annex III of EU AI Act. Ther list encompasses 4 institutions: *Office of the Equal Opportunities Ombudsperson; The Seimas Ombudsmen's Office; The Office of the Ombudsperson of Child's Rights; The Office of the Inspector of Journalist Ethics*. The first two institutions will also coordinate other bodies functioning in the field of human rights protection (in Lithuania there are about 100 of them).

To promote democratic values and human rights on a global scale in the development and use of digital technologies, Lithuania also underlines the importance of the **Vilnius Convention** – the Council of Europe Framework Convention on Artificial Intelligence signed in Vilnius on September 5, 2024. It is the first international legally binding treaty establishing a global minimum standard for the protection of human rights from the risks posed by AI.

(iv)

[26] Available in Latvian at: https://titania.saeima.lv/LIVS14/saeimalivs14.nsf/0/2902CD41AFAACBC7C2258BF6002FD6BA?OpenDocument.

Education

Ministry of Education, Science and Sport to coordinate AI in education - Coordination through Working Groups and cooperation with the Lithuanian AI Association.
National Agency for Education - Consultations & training for teachers –
EdTech Centre - Providing information and access to digital resources through Education Portal (focus on digital teaching materials), provision of teaching equipment, testing of EdTech solutions.
Digital Education Guidelines for schools : https://emokykla.lt/upload/media/public/Kita-aktuali-medziaga/Skaitmeninio%20%C5%A1vietimo%20gair%C4%97s%20_%20galutinis%20(2).pdf

Social Services and Welfare and Labour and Employment:
Lithuania is currently in the process of transposing the EU Platform Work Directive into its national law. The new regulations will ensure that individuals engaged in platform work cannot be terminated based on decisions made solely by algorithms or automated systems. Instead, digital labour platforms must implement human oversight for significant decisions that directly impact platform workers. Additionally, the directive introduces stronger data protection measures for platform workers. Digital labour platforms will be prohibited from processing certain types of personal data, including information about an individual's emotional or psychological state and personal beliefs.

AI is being applied in the social services sector in Lithuania, although the implementation of its frameworks is still evolving. Several agencies under the Ministry of Social Security and Labour of the Republic of Lithuania (hereinafter referred to as the Ministry) utilize virtual customer service assistants. For instance, AI solutions have been implemented in the Employment Service under the Ministry of Social Security and Labour to improve the quality and accessibility of the services provided. A chatbot has been introduced at the Employment Service to answer client inquiries on the following topics: registration with the Employment Service, employment of foreigners, support for business creation, support for training, and wage subsidies. Chatbot uses AI (natural language processing) technology to better predict the intent of client and provide most accurate answer. The statistical profiling model evaluates the probability of a client registered with the Employment Service securing employment within a 12-month period. The results of this model are used as an evidence-based support mechanism for Employment Service front-line counsellors, who make final decisions on what services might be provided to which client, depending on their distance to the labour market. Currently, AI-based solutions used in the Employment Service operate without using personal data (or use anonymized data), and no decisions affecting users are made during these processes. From the initiation of the projects, the risk of encountering ethical issues was assessed as insignificant, and no signs indicating potential bias or discrimination were observed during testing or during live operation.

In today's rapidly evolving technological landscape, artificial intelligence (AI) has become an indispensable tool for enhancing productivity and efficiency in the workplace. The Ministry of Social Security and Labour of the Republic of Lithuania (hereinafter referred to as the Ministry) has recognized the potential of AI and has established specific guidelines for its use by employees. These guidelines are incorporated into a separate chapter No XVI in the updated Rules[27] for the Processing of Personal Data in the Ministry of Social Security and Labour of the

[27] Asmens duomenų tvarkymo Lietuvos Respublikos socialinės apsaugos ir darbo ministerijoje taisyklės, patvirtintos Lietuvos Respublikos socialinės apsaugos ir darbo ministro 2018 m. spalio 31 d. įsakymu Nr. A1-610 (Lietuvos Respublikos socialinės apsaugos ir darbo ministro 2024 m. gruodžio 27 d. įsakymo Nr. A1-934 redakcija)

Republic of Lithuania. This ensures that AI is used responsibly and in compliance with relevant regulations. Employees are granted the right to utilize free AI technology tools such as ChatGPT, DeepL, Claude, and Microsoft Copilot while performing their functions. These tools can significantly enhance various aspects of their work, from drafting documents to automating routine tasks. However, it is crucial that these tools are used only for lawful purposes and in compliance with Regulation (EU) 2016/679, which governs the protection and processing of personal data. The use of AI tools must align with the principles outlined in Resolution No. XIV-2620 of the Seimas of the Republic of Lithuania, dated May 9, 2024. This resolution emphasizes the importance of ethical AI usage in the public sector, ensuring that AI technologies are employed responsibly and transparently. Employees must be aware of these principles and integrate them into their daily operations. To maintain transparency and accountability, only documents that are publicly available in the Register of Legal Acts and on the Ministry's website may be used for work functions involving AI. This ensures that sensitive or confidential information is not inadvertently exposed or misused. Information security is paramount when using AI technologies. It is recommended that AI tools be employed primarily for internal and external communication, such as preparing press releases and text messages, and for drafting internal procedures without disclosing specific institutional details. Additionally, AI can be used for creating documents intended for internal use and for daily tasks that do not pose a threat to data security or legal obligations, such as preparing slides and creating images.

MALTA / *MALTE*

Yes, Malta has implemented certain measures, guidelines, or practices which aim to address potential impacts on HR by businesses involved in the AI system lifecycle, and to provide remedies when such impacts occur.

Details:

The Malta Digital Innovation Authority (‘MDIA’) has implemented the Technology Assessment Recognition Framework (‘TARF’) and the MDIA AI Self-Assessment Toolbox. The Malta Information and Technology Agency also built the Generative AI Tool Usage Policy.

The TARF established by the MDIA provides is a tiered framework designed to provide varying degrees of recognition to a wide range of technologies, including AI, aligning with international standards and industry best practices. TARF is targeted towards owners or operators of technology solutions, who want to assess and obtain recognition for their technology-related controls. The framework is flexible, allowing applicants to choose what they want to be assessed against, with different assessment levels building on each other for higher trust levels.

The MDIA AI Self-Assessment Toolbox intended to provide generic guidance to users in understanding potential classifications under the European Union's Regulation (EU) 2024/1689, the Artificial Intelligence Act.

The Generative AI Tool Usage Policy covers the use of generative AI tools involving input of Government data for machine learning and/or as support for any form of decision-making purposes within the Public Administration.

The MDIA has adopted the practice of conducting roundtable meetings and presentations regarding the topic of AI and fundamental rights.

MONTENEGRO / *MONTÉNÉGRO*

As regards the second question, I inform you that the Ministry of Public Administration of Montenegro is competent for drafting and monitoring the implementation of strategic documents in the field of artificial intelligence in Montenegro and for managing artificial intelligence policy in accordance with international standards and practice of the European Union.
According to the information provided by that Ministry no specific measures, guidelines, or practices which aim to address potential impacts on human rights by businesses involved in the artificial intelligence systems lifecycle have been implemented in Montenegro by this moment. However, the Strategy for artificial intelligence of Montenegro is planned to be developed this year, which Strategy will include all spheres of society, it is expected that the Action plan for the implementation of that Strategy will define the obligation of developing the aforementioned measures, guidelines, or practices.

MONACO

Non.
Bien que l'intelligence artificielle ne fasse pas encore l'objet de décision spécifique des tribunaux à Monaco, le Gouvernement travaille actuellement à l'encadrement de son intégration notamment dans le domaine de la sécurité publique avec le projet de loi n° 1.087 relative à l'utilisation de la vidéoprotection et de la vidéosurveillance des lieux accessibles au public pour la détection, la recherche et l'identification des personnes recherchées ou signalées au moyen de systèmes d'identification biométrique à distance.

NETHERLANDS / *PAYS-BAS*

As an EU member state, the Netherlands has the EU AI Act, which contains rules that aim to address potential impacts on human rights by businesses.

POLAND / *POLOGNE*

Poland is currently actively working on aligning its national policies with the European Union's Artificial Intelligence Act (AI Act) to address human rights implications associated with AI systems.

(i) Legal and Policy Frameworks:

- In October 2024, Poland's Ministry of Digital Affairs designated specific authorities responsible for enforcing fundamental rights protections under the AI Act. This initiative underscores Poland's commitment to ensuring that AI systems adhere to human rights standards throughout their lifecycle.

- Poland has endorsed the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS 225 - Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law). The Convention was signed by the European Commission on 5 September 2024 on behalf of the European Union. The Convention is consistent with the EU Artificial Intelligence

Act, as well as with other European Union legislation, and covers a number of key concepts contained in the Act on Artificial Intelligence.

- Poland has begun legislative work to enable the proper implementation of the AI Act. The draft Act on Artificial Intelligence Systems aimed at introducing regulations for the application of the regulation into the national legal order has been entered in the list of legislative and programme works of the Council of Ministers. The public consultation of the draft Act (the Draft) has now been completed.

  It is envisaged to establish a new market oversight body for AI models and systems, which will be the Artificial Intelligence Development and Safety Commission. It is proposed to designate the minister responsible for information technology as the competent authority for the notification of conformity assessment bodies and as the notifying authority.

- Poland has a 'Policy for the Development of Artificial Intelligence in Poland from 2020' adopted by a Resolution of the Council of Ministers. The Policy describes the actions Poland should implement and the goals it should achieve in the short term, medium term (until 2027) and long-term (after 2027), aimed at the development of Polish society, Polish economy and Polish science in the field of AI.

  All objectives and tools are divided into six areas:

  Ministry of Digitalisation is currently underway to revise the current AI Policy aligning its content with current challenges and technological changes. The AI Policy will also feed into the National Digitalisation Strategy under development.

- The Ministry of Digitalisation on 23 September 2024 published recommendations for the use of generative AI in public administration.

- Poland adopted the 'Recommendation on the Ethics of Artificial Intelligence' on 23 November 2021 by resolution of the 41st session of the UNESCO General Conference.

- Additionally, Poland's AI strategy emphasizes the development of a holistic AI ecosystem, aiming to meet objectives that align with international standards, such as the OECD AI Principles and the UN Guiding Principles on Business and Human Rights. It emphasizes ethical considerations in AI deployment, particularly in high-risk areas such as healthcare, public administration, and law enforcement.

(ii) Monitoring Compliance and Providing Remedies:

The AI Act proposes new approach based on risk assesment and introduces classification of AI systems by risk categories (prohibited, high, limited and minimal risk).
It is worthy to mention that the first two categories prohibited and high risk establish rules under which businesses must:

- Conduct human rights impact assessments to identify and mitigate risks.
- Implement data governance frameworks that reduce bias and protect privacy.
- Ensure systems are auditable, transparent, and explainable to end-users and regulators.

and are prohibited from as follows:

using subliminal or manipulative techniques to distort behaviour and decision-making
- using AI systems that exploit the vulnerabilities of specific groups, such as those based on age, disability, or socio-economic status
- using AI systems that evaluate or classify individuals based on their social behaviour, leading to social scoring
- using AI to predict criminal offenses solely based on profiling or assessing personality traits
- creating and expanding of facial recognition databases through untargeted scraping of images from the internet or CCTV footage
- using AI systems to infer emotions in workplaces and educational institutions, with exceptions for medical or safety purposes
- using AI systems that categorize individuals based on sensitive biometric attributes, such as race or sexual orientation.

As mentioned above the AI Act mandates that providers of high-risk AI systems implement risk management systems, conduct regular compliance audits, and ensure transparency and safety. Distributors and importers are also required to ensure that the AI systems they bring to market meet all legal requirements, facing similar liability to suppliers in the event of violations. Users are obliged to monitor the operation of systems, report problems, and ensure that the technologies are used according to their intended purpose and supplier recommendations. These measures are designed to uphold human rights standards in AI applications and provide mechanisms for individuals to seek remedies when violations occur.

Furthermore, the AI Act enhances rights under the General Data Protection Regulation (GDPR), emphasizing transparency and effective human oversight of AI systems. This enhancement facilitates better monitoring of business compliance with human rights standards in the context of AI.

In summary, Poland is in process of implementation of specific measures and designating authorities to enforce the AI Act, ensuring that businesses involved in the AI lifecycle address potential human rights impacts and provide remedies when such impacts occur.

(iii) Corporate Responsibility and Stakeholder Engagement in AI:

While specific practices are still emerging, Polish companies are increasingly recognizing the importance of Corporate Social Responsibility (CSR) in the context of AI. Research indicates that CSR projects are becoming integral to public relations activities, though they are not yet a specialized focus for many agencies. This trend suggests a growing awareness of the need for responsible AI practices and meaningful stakeholder engagement.

Additionally, Poland's AI strategy emphasizes the development of a holistic AI ecosystem, aiming to meet objectives that align with international standards.

(iv) Sector-Specific Measures and Guidelines:

- Poland is in the process of aligning its national policies with the AI Act to address human rights implications associated with AI systems. The document introduces uniform rules for the creation and use of AI systems based on risk assesment, aiming, in order to balance innovation with safety. In the polish healthcare sector, while AI is already in use, there are

currently no specific national guidelines for its application. This lack of regulation is not unique to Poland and reflects a broader international context. Similarly, in the financial sector, there are no specific national laws governing AI use. However, existing regulations and guidelines from authorities, such as the Polish Financial Supervision Authority (KNF), may impose certain restrictions, as AI systems in finance must comply with the Banking Law and other financial regulations overseen by KNF. As the AI landscape evolves, it is anticipated that Poland will continue to develop and implement sector-specific measures to ensure that AI applications adhere to human rights standards across various public governance sectors.

- Working Group on Artificial Intelligence (GRAI) - Ethics and Legal Subgroup under the Ministry of Digitalisation prepared a 'Report - Recommendations for the application of AI in the Judiciary and Public Prosecution' (Warsaw 2023), which contains recommendations on the development of AI, its legal framework, legislative changes and good practices.

  The recommendations are of a general, specific and implementation nature. The essence of the general recommendation is the development of databases on the basis of which software will operate based on AI systems. The essence of the general recommendations is the development of databases on the basis of which the software will operate based on AI systems. The general recommendations concern: electronic writ of payment proceedings, portal of common court decisions, PESEL-SAD (digital database), digitalisation of court files and the PROK-SYK system (digital database). Electronic writ-of-payment proceedings, supported by an ICT system, is the best digitalised form of proceedings in Poland.

  Specific recommendations concern: automatic transcription of trial proceedings into written minutes, a system for the creation of cumulative sentences, the wider introduction of a court chatbot to complement the work of the customer service, which would provide information on court procedures and the status of the case, systems for handling requests for exemption from court costs and granting of ex officio representation, searches for similar cases and the creation of draft justifications. Specific recommendations further relate to: the register of succession and the notarial register of wills, the analysis of the of court staffing and workload and court statistics, live translation of hearings, the use of translators for the translation of court letters, and a system to analysis of criminal notices and evaluation of evidence in pre-trial proceedings.

  Implementation recommendations assume: the creation of a Centre for Robotisation of Processes at the Ministry of Justice, to submit requests for robots to prepare analyses of specific categories of cases and prepare a report for the judge. The centre would also serve to automating the administrative activities of the courts. As part of the implementation recommendations also the need to merge systems already in place. Attention was drawn to the risks in the implementation of AI in the judiciary, in particular related to the random case allocation system introduced in 2018. The report indicated that AI systems that learn from databases should be subject to procedures for estimating the risk of security breaches of machine learning, in particular with regard to ensuring the proper management of sensitive data.

- It is also worth to mention about the digital arbitration courts in Poland. There are actually five digital arbitration courts: Ultima Ratio, CODR, OAC, the Arbitration Court at the Polish Confederation of Private Employers 'Lewiatan', and ENOIK as an example of a Polish company that has created an arbitration court, which uses AI algorithms to resolve payment

disputes between entrepreneurs. According to data from ENOIK's entity page, arbitrators in the process of resolving legal disputes are supported by an algorithm trained on the basis of hundreds of thousands of cases recognised by common courts. As a result, it is able to guarantee the resolution of a legal dispute within 40 working hours of receiving a set of documents. Filing a claim in the ENOIK Arbitration Court allows entrepreneurs many times faster to obtain a judgment on their receivables from dishonest counterparties, reducing the risk of liquidity problems.

- White Paper AI in Clinical Practice has been prepared by Ministry of Health as well as the eHealth Development Programme 2022-2027.

SAN MARINO / *SAINT-MARIN*

No.

SERBIA / *SERBIE*

The Republic of Serbia is in the process of implementing legislature concerning artificial intelligence.

It has implemented a Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025[28], Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2025-2030[29] and Ethical Guidelines for Development, Implementation and Use of Robust and Accountable Artificial Intelligence[30] (hereinafter: the Guidelines).

The Strategies are in line with the European Artificial Intelligence Initiative[31], which sets out the European Commission's artificial intelligence policy. In this context, the Republic of Serbia, as a candidate for EU membership, but also as a participant in the European Union Framework Program for Research and Innovation, seeks to provide the necessary extent of compliance with the European Union, which will enable full integration into the European Research Area and closer cooperation.

The Strategies set out the aim of artificial intelligence application in an ethical and safe manner. This is further concretized in the Guidelines, which provide for the principles of dignity, fairness and prohibition to cause damage. Special attention is devoted to the issues of privacy, personal data protection and data management; transparency; diversity, non-discrimination and equality; social and environmental wellbeing; and accountability.

The Guidelines reflect the principles set out in the UNESCO Recommendation on the Ethics of AI of November 2021 as well.

---

[28] https://www.media.srbija.gov.rs/medsrp/dokumenti/strategy_artificial_intelligence.pdf
[29] https://www.srbija.gov.rs/vest/en/241045/strategy-for-ai-development-until-2030-adopted.php
[30] https://www.ai.gov.rs/extfile/en/471/Ethical%20guidelines%20for%20development%20implementation%20and%20use%20of%20robust%20and%20accountable%20AI.pdf
[31] "Artificial Intelligence for Europe", COM(2018) 237 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

(i) Mechanisms for monitoring and assessing business compliance with human rights standards in the context of AI, and mechanisms through which rights holders may seek remedies.

The Government of the Republic of Serbia has established the Council for Artificial Intelligence in 2024. Its task is to align and coordinate activities related to implementing the strategic framework for developing artificial intelligence, as announced in the Official Gazette.

The Council's tasks also include monitoring the implementation of planned measures and activities, observing the state, needs, and standards of AI development and application in Serbia and globally. The Council has an advisory role, preparing proposals, recommendations, and standards, providing opinions, and expert explanations on all issues related to the development and application of AI in Serbia.

The Council organizes and monitors the preparation of laws and regulations concerning the development and application of AI in Serbia.

SLOVAKIA / *SLOVAQUIE*

Since 2021, the Minister of Investments, Regional Development, and Informatization of the Slovak Republic has had an advisory body known as the Permanent Commission for Ethics and Regulation of Artificial Intelligence (CERAI). The role of CERAI is to assess the ethical, socio-political, and legal issues related to the research, development, deployment, and use of technologies that incorporate AI elements and systems. For example, CERAI has prepared the following opinions: Opinion on the importance of a responsible approach when deploying artificial intelligence in the conditions of Slovak public administration and Opinion on the ethical issues of generative artificial intelligence and large language models. The opinions of this commission are available online: https://mirri.gov.sk/sekcie/investicie/digitalne-inovacie/stala-komisia-pre-etiku-a-regulaciu-umelej-inteligencie/informacie-o-komisii/

According to the information provided by the Ministry of Investment, Regional Development and Informatization of the Slovak Republic, that ministry elaborated the “Principles of Safety in the Use of Artificial Intelligence Systems,” which must be followed when using AI at work and informed its employees about it. This guidance also addresses the protection of personal data and encourages employees to use AI for ethical and democratic purposes.

In the purpose of ensuring the compliance with ethical principles in the field of AI, in September 2024, Ministry of Investment, Regional Development and Informatization of the Slovak Republic in a letter to UNESCO expressed interest in participating in the RAM (Readiness Assessment Methodology) tool. This tool aims to assess countries' readiness for AI and will provide support in implementing UNESCO's recommendations in the field of AI.

SPAIN / *ESPAGNE*

Response from the Secretary of State for digitalisation and AI

Regarding the second question, Spain has not implemented specific measures, guidelines, or practices aimed at addressing potential human rights impacts by businesses involved in the AI systems lifecycle. Additionally, no formal mechanisms exist to allow rights holders to seek remedies in this context.

Therefore, we cannot provide relevant information for this section.

Response from the State Attorney General's Office

In Spain, the General State Attorney's Office is developing a pilot project for an **application based on generative AI,** named TEMIS, to generate draft responses in an automated manner to the judicial claims to which the legal service of the Spanish state must respond, based on the established competencies.

TEMIS applies advanced Natural Language Processing (NLP) techniques to analyze the text of the legal claims. Every time a new claim is submitted, the tool compares it with our historical documentary base, **thanks to the artificial intelligence engine, and offers** the Spanish General State Attorney's Office a recommendation for a similar historical claim. The State's attorney analyzes whether the recommendation is optimal and, if satisfied, can ask the tool to **automatically generate a draft response in an editable file**.

The Spanish General State Attorney's Office continues to be the one who controls the entire process, since both the recommendation of a similar historical claim and the generation of the draft response require human action, validation and supervision in all cases. **Therefore, there is no automation in decision making, but rather support for our daily work.**

In order to **protect the human rights, and also with the aim to comply with the Spanish and European legislation with impact in the public governance sector**, the Spanish General State Attorney's Office have implemented the following measures in the TEMIS application scope:

1) Every personal data managed by the application has been anonymized.

2) A data protection impact assessment has been conducted, following the instructions of **General Data Protection Regulation framework (GDPR**). This assessment has been validated by the PILAR application, aligned with security standards and regulations, such as the National Security Framework and GDPR, to ensure that information systems meet the required security and data protection standards.

3) A risk assessment has been carried out following the guidelines from **National Security Framework** (link). With this action, the Spanish General State Attorney's Office has obtained a risk classification based on their impact and likelihood, and a report for implementing appropriate security measures to mitigate these risks.

4) In addition to this, the Spanish General State Attorney's Office is working, from September 2024, **to be certified by the National Security Framework**, **as secure public governance actor**, and TEMIS is also included in this scope. This means that the Spanish General State Attorney's Office must comply with the requirements set out in the Security Framework, which cover aspects such as information protection, service continuity, incident management, and staff training.

A) Summary of the the Data Protection Impact Assessment and Risk Analysis:

1. **Data Protection Impact Assessment:**

This assessment involved analyzing how the assets that are part of TEMIS impact various dimensions related to the availability, integrity, and confidentiality of the data processed by this application, as well as addressing a specific dimension for personal data.

Assets are understood to include everything from the IT infrastructure supporting the TEMIS application to the data itself (including personal data) contained in the documents managed by the application to provide an automated response to a new incoming request.

To carry out this assessment , PILAR system has been used. This tool belongs to the National Cryptologic Centre, depending on National Intelligence Centre.

According to the impact assessment conducted using the PILAR tool, the risks associated with each of these assets across the mentioned dimensions are measured on three levels: low, medium, and high.

In general terms, the TEMIS application presents a **medium risk** due to the impact of the risks detected across its various dimensions.

Below is an example of some of the threats identified and the level of risk associated with an impact on the "data integrity" dimension:

Threat	**Risk level**
Errors in maintenance/updates of software	Medium
Spread of malicious software	Medium
Identity impersonation	Medium

2. **Security Risk Analysis (National Security Framework)**

Following the instructions of **the National Security Framework, regulated in Spain by Royal Decree 311/2022, a risk analysis has been conducted concerning the TEMIS Information System**. This analysis is more focused on technical and technological aspects, but undoubtedly contributes to ensuring data protection and the respect for human rights.

As with the Data Protection Impact Assessment, the dimensions analyzed have been the availability, integrity, and confidentiality of the data processed by this application, as well as addressing a specific dimension for personal data.

In this analysis, technological or IT threats that could negatively impact the service delivery and the IT assets supporting it have been evaluated.

In this regard, this document describes, as an example, some of the threats established by the National Security Framework, which have been considered in this risk analysis:

- Injection of malicious code (through a logical boundary)
- Information extraction (through a logical boundary)
- Unauthorized access
- Identity impersonation

The result of this analysis shows a medium-level risk concerning the considered threats and assets.

B) Next actions to develop

As a consequence of both analyses, a set of measures will be implemented to reinforce security in the TEMIS application, therefore guaranteeing data protection.

To name some of those contemplated:

1) Safe access policy to the application following the recommendations of the National Security Scheme, identifying each member of the General State Attorney's Office that uses it.

2) Traceability and auditing of the actions that TEMIS users take in the application.

3) Security audit of the application code to detect gaps that may compromise illegitimate access.

With these and other measures, the Spanish General State Attorney's Office aims to guarantee respect for human rights, ensuring that user information is handled with privacy, integrity and transparency

SWITZERLAND / *SUISSE*

There are currently no specific and horizontal measures addressing potential impacts by businesses. However, there are sectoral measures (see further below) as well as measures for the public administration (see further below as well). Furthermore, in November 2023, the Swiss Federal Council has mandated an overview of possible regulatory approaches for Switzerland.
The analysis will build on existing Swiss law, identify possible regulatory approaches for Switzerland that are compatible with international developments such as the EU AI Act and the Council of Europe's AI Convention. The analysis will examine the regulatory requirements with a particular focus on compliance with fundamental rights. The technical standards and the financial and institutional implications of the different regulatory approaches will also be taken into account.
The report will be published shortly, presumably mid-February 2025.
In detail:

The legal or policy frameworks in place, including specific obligations or guidelines aligned with international standards (e.g., UN Guiding Principles, OECD Guidelines) for businesses to address human rights risks across the AI lifecycle

There is currently no specific legal or policy framework in place for businesses. However, Switzerland is currently in the process of assessing its legal framework and deciding whether further action is needed (see above). A decision is expected in early 2025.
The updated Swiss National Action Plan on Business and Human Rights 2024-2027 includes a measure for strengthening the uptake of the UN Guiding Principles in the digital space and new technologies through efforts aimed at companies and states to promote guidelines such as those developed under the UN B-tech project.

Mechanisms for monitoring and assessing business compliance with human rights standards in the context of AI, and mechanisms through which rights holders may seek remedies
See above

Examples of practices that enable corporate responsibility to respect human rights and meaningful stakeholder engagement in the context of AI (for e.g. advisory forums or regular meetings)
See above

Sector-specific measures, guidelines, or practices concerning the following public governance sectors
Yes, there are several measures. As mentioned above, Switzerland will soon publish a comprehensive overview of these measures. The contributions below are summarized extracts from this publication.

Law Enforcement and Public Safety
The Federal Office of Police (fedpol) is currently in the process of updating its automated fingerprint identification system (AFIS). AFIS is a siloed IT system that contains information for the biometric identification of individuals (e.g., fingerprints and palm prints). The new system is planned to include facial image matching for wanted persons, but these images will not be automatically compared in real time with surveillance camera images.

Administration of Justice
We currently do not have specific information on this area.

Healthcare
The Federal Office of Public Health (FOPH) is currently drawing up a comprehensive overview of the possible use and regulation of AI systems in the healthcare sector. This also takes into account overlaps and responsibilities within the federal administration and in the international environment. For example, AI is relevant in the area of image recognition by medical devices, which will have an impact on the supervisory activities of Swissmedic and, as currently assessed, will require legislative amendments.

Education
In June 2021, the Swiss Conference of Cantonal Ministers of Education and the State Secretariat for Education, Research and Innovation (SERI) jointly committed to establishing clear rules for data processing in the education sector. The stated goal is to develop a data usage guideline (focusing on primary and secondary education) by June 2025. This should guarantee that data in the education system is processed securely and ethically throughout Switzerland, while also enabling targeted use.

The specialist agency Educa has been commissioned to create a programme for data usage projects. This should help to identify the needs of the various stakeholders and the associated opportunities and challenges. The findings will be incorporated into future data use policy. One of the projects registered in the programme so far is concerned with the use of algorithms and AI in education. The aim is to identify and analyse the potential need for regulation. On this basis, possible regulatory approaches will be outlined and discussed with the relevant stakeholders.
As part of this mandate, Educa, together with the Center for Information Technology, Society and Law (ITSL) at the University of Zurich, has conducted a study on the legal framework for the development and use of AI in the Swiss education sector. The aim of this study is to determine how AI applications can be used in the field of education without harming the people involved or infringing on their rights. The results of the study were published in summer 2024[32]. Based on the study, Educa concludes that many of the questions raised by AI – especially those related to responsibilities – can be answered with existing data protection regulations. At most, there would be a need for action in school legislation. In particular, it would be necessary to examine whether the general provisions of these laws are sufficient when AI systems process personal data that is particularly worthy of protection.

Social Services and Welfare
We currently do not have specific information on this area.

Immigration and Border Control
The legal framework governing the Federal Office for Customs and Border Security (FOCBS) is being updated. The new framework will introduce so-called automated controls which would allow for declarations of goods to be checked, for example, by means of digital verification of permits or quantity restrictions. Automated controls are also to be used in passenger transport within the European legal framework.
This new piece of legislation will place strict requirements for the transfer of data to partner authorities or for their storage, archiving and destruction. In addition, high demands are placed on internal quality assurance. In particular, the FOCBS must continuously review its practices relating to data processing with regards to their compliance with data protection regulations as well as the protection of human rights. The relevant provision[33] expressly mentions prohibition of arbitrariness and discrimination when processing data in the context of risk analyses and of profiling and high-risk profiling, as well as assessing the use of AI systems during their entire lifecycle.

Labour and Employment
The Federal Personnel Act (FPA), which governs the employment relationship between the Confederation and its staff, is currently being updated, in particular to create the adequate legal basis for allowing profiling and high-risk profiling (e. g., when looking for candidates on social media platforms). The updated provisions would also be relevant for the potential future use of AI systems in areas of human resources other than staff recruitment, for the targeted promotion and long-term retention of employees and for staff development. The guidelines on artificial intelligence for the federal government (see below) will also be taken into account.
Housing and Urban Planning
We currently do not have specific information on this area.

Taxation
We currently do not have specific information on this area.

[32] Available in German: https://www.educa.ch/de/aktuelles/educa-dossier/ki-der-bildung
[33] Art. 170 of the draft legislation: https://www.fedlex.admin.ch/eli/fga/2022/2725/fr#art_170

Democratic Processes
We currently do not have specific information on this area.

Public Administration
Switzerland has guidelines on artificial intelligence for the federal administration since November 2020[34]. The guidelines provide the federal administration (and the bodies that carry out administrative tasks for the federal government) with a shared framework and are intended to ensure a coherent policy with regard to AI. The guidelines do not apply to businesses or other actors outside of the federal administration.
The guidelines comprise seven key principles (summarised below) and are subject to periodic review:

- **Human-centric:** The dignity and well-being of people and the common good should be the top priority when developing and using AI systems in the federal administration. Particular importance is attached to the protection of fundamental rights.
- **Framework for the development and application of AI:** The federal government will continue to ensure the best possible framework conditions so that the opportunities offered by AI can be leveraged, while mitigating any potential risks. Switzerland should continue to develop into a leading location for research and application, as well as for companies in the field of AI.
- **Transparency, traceability and explainability:** AI-based decision-making processes should be designed in such a way that they are verifiable and comprehensible.
- **Accountability:** In order to be able to clarify responsibilities in the event of damage, an accident or an infringement of the law, liability must be clearly defined when using AI systems. Accountability must not be delegated to machines.
- **Security:** AI systems must be designed to be secure, robust and resilient in order to have a positive impact and to avoid being susceptible to misuse or abuse.
- **Active participation in the governance of AI:** Switzerland should actively participate in the global governance of AI and contribute to the development of global standards and norms in line with its interests and values.
- **Involvement of all affected national and international actors:** Switzerland should work to ensure that all relevant stakeholders are included in the debates and the political decision-making processes on the governance of AI.

TÜRKIYE

Responses of Digital Transformation Office (DTO)

[34] In English: https://www.sbfi.admin.ch/dam/sbfi/en/dokumente/2021/05/leitlinien-ki.pdf.download.pdf/leitlinien-ki_e.pdf

Has your country implemented any specific measures, guidelines, or practices which aim to address potential impacts on human rights by businesses involved in the artificial intelligence systems lifecycle, and to provide remedies when such impacts occur?

The Personal Data Protection Authority has published the "Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence"[35] document, which includes recommendations for developers, manufacturers, service providers and decision makers operating in the field of artificial intelligence for the purpose of protecting personal data within the scope of the Law No. 6698 on the Protection of Personal Data (KVKK)[36].

i. **The legal or policy frameworks in place, including specific obligations or guidelines aligned with international standards (e.g., UN Guiding Principles, OECD Guidelines) for businesses to address human rights risks across the AI lifecycle.**

With the National Artificial Intelligence Strategy (NAIS)[37] published by the Digital Transformation Office (DTO) of the Presidency of the Republic of Türkiye and the Ministry of Industry and Technology in August 2021, it is stated that Türkiye is a stakeholder of the human-centered AI principles determined by the OECD, G20, EU and UNESCO and adopts the values and principles of "trustworthy and responsible AI".

The above-mentioned "Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence" are considered as an important guideline for the implementation of the basic principles set by the OECD and the UN.

ii. **Mechanisms for monitoring and assessing business compliance with human rights standards in the context of AI, and mechanisms through which rights holders may seek remedies.**

The Personal Data Protection Authority (KVKK) is tasked and authorized to decide on complaints regarding issues such as unauthorized data processing, data leakage and privacy violations that occur within the framework of the processing of personal data in AI systems, and upon complaint or upon learning of the alleged violation, to examine ex officio whether personal data is processed in accordance with the law in matters falling within its jurisdiction and to take temporary measures in this regard when necessary.

The Human Rights Investigation Commission of the Grand National Assembly of Türkiye (TBMM) has duties such as observing respect for human rights and examining individual applications alleging violation of human rights. The Commission's field of work consists of human rights protected by the Constitution, laws, documents such as the Universal Declaration of Human Rights (UNHR) and the European Convention on Human Rights (ECHR).

[35] https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler
[36] https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5
[37] https://cbddo.gov.tr/SharedFolderServer/Genel/File/TRNationalAIStrategy2021-2025.pdf

As a result of the applications made to the Human Rights and Equality Institution of Türkiye (TİHEK) in case of violation of the prohibition of discrimination, the Institution has the authority to impose administrative fines.

Apart from all these remedies, the judicial remedy is always open in case of human rights violations arising from artificial intelligence systems.

In addition, the preparation process of the “Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law” (the Convention), the first binding international convention on artificial intelligence by the Council of Europe, has been carried out from the very beginning with the active participation of our country. The Convention was opened for signature on September 5, 2024 and the process for its signature is being followed by Türkiye. In addition, the preparation of human rights, democracy and rule of law impact assessment documents, which are complementary to the Convention, is ongoing. The Convention imposes responsibilities on Parties in terms of implementing internationally recognized fundamental principles and stipulates obligations on the protection of human rights, the integrity of democratic processes and respect for the rule of law. Principles such as human dignity and individual autonomy, transparency and oversight, equality and non-discrimination, accountability and responsibility, privacy and protection of personal data, and trustworthiness, which are also recognized by the Convention, are in line with principles accepted by international organizations such as the OECD and UNESCO.

iii. Examples of practices that enable corporate responsibility to respect human rights and meaningful stakeholder engagement in the context of AI (for e.g. advisory forums or regular meetings).

Türkiye became a part of the Hiroshima AI Process Friends Group[38], a voluntary framework of countries supporting the spirit of the Hiroshima AI Process by the G7, toward achieving safe, secure, and trustworthy AI that commit to the implementation of the "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems"[39] and “Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems”[40].

In this context, or country regularly participates in meetings organized for the implementation and review of the relevant documents and submits its comments.

iv. Any sector specific measures, guidelines, or practices concerning the following public governance sectors

- **Law Enforcement and Public Safety**
- **Administration of Justice**

[38] https://www.soumu.go.jp/hiroshimaaiprocess/en/supporters.html
[39] https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document05_en.pdf
[40] https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document04_en.pdf

- **Healthcare**
- **Education**
  - "Ethical Guidance on the Use of Generative Artificial Intelligence"[41] published by the Council of Higher Education (CoHE)
- **Social Services and Welfare**
- **Immigration and Border Control**
- **Labour and Employment**
- **Housing and Urban Planning**
- **Taxation**
- **Democratic Processes**
- **Public Administration**
  - Resolution No. 2024/108 on the "Principles of Ethical Conduct to be Followed by Public Officials in the Use of Artificial Intelligence Systems"[42] published by the Public Officials Ethics Board.

Responses of the Ministry of Justice

There are many examples where artificial intelligence (AI) applications are used today in the justice system and court management. In accordance with the National Artificial Intelligence Strategy, in April 2020 the Department of Big Data and Artificial Intelligence has been established within the IT Department of the Ministry of Justice. Through the integration of updated artificial intelligence technologies and big data applications into their system, it is aimed that judges, prosecutors, presidents and members of courts of first instance and appeal are assisted so as to minimize errors during the legal proceedings.

With a view to preventing mistakes and entering incomplete information in files during the investigation stage, improving the accuracy of judicial statistical data and reports requested by reviewing bodies, and estimating information relating to terror organizations through AI and matching them with the information stored in the database, AI models have been developed by the IT Department of the Ministry of Justice and installed to the UYAP system.

Moreover, it has been ensured that the information contained in court notices are entered in files using AI. It has been possible to detect the barcode with artificial intelligence for collective and automatic recording of PTT (Postal Service) court notices to the relevant file and to automatically fill in the status, date and other information of the notification with the integration with PTT. The project has ensured saving time and workforce and that human errors are minimized.

In addition, AI is also used in the UYAP system for identifying the workload of chambers in courts of appeal. In the event that the appeal chamber considers, during the preliminary examination stage that it lacks jurisdiction, it refers the file to the chamber which has jurisdiction. It is a well-known fact that the proceedings are delayed if the file is submitted to the wrong chamber. In this context, an artificial intelligence model has been developed by taking into account

[41] https://www.yok.gov.tr/Documents/2024/yapay-zeka-kullanimina-dair-etik-rehber.pdf
[42] https://www.etik.gov.tr/media/oekdkifu/yapay-zeka.pdf

the 50 most common issues in which a decision of non-jurisdiction is rendered. As a result, 88 percent success has been achieved in submitting the files to the correct chamber.

Work is in progress for the development of the AI application "*Söyle Yazsın*" to convert voice into text during the document preparation works in UYAP, as well as smart assistant and AI guide applications which will provide information on the legal proceedings within the lawyer and citizen portals.

An artificial intelligence model is under development for the identification of criminal miscellaneous document type in order to determine the different types of work files in criminal courts and to open the arrest, judicial control and removal of judicial control decisions in the correct file type.

With this project, it will be ensured that the workflow is formed in the accurate way by preventing the user from inaccurate selection of the incoming request or the sender unit from selecting the wrong document.

In 2023, it was announced that within the framework of the "Project for Strengthening the Institutional Capacity of the Court of Cassation", implemented together with the Council of Europe, executive summaries of landmark decisions shall be made accessible promptly using AI. An AI-assisted Case-Law Center has been established to make the case-law of the Court of Cassation widespread.

Finally, no judicial decision has been found which addresses the ethical and legal dimensions of AI applications.

UNITED KINGDOM / *ROYAUME-UNI*

i. AI Management Essentials (AIME) is a self-assessment tool aimed primarily at small-to-medium enterprises. It is designed to provide clarity to organisations around practical steps for establishing a baseline of good practice for managing artificial intelligence (AI) systems that they develop and/or use. The tool distils key principles from existing AI-related system management frameworks and standards including ISO/IEC 42001, the NIST Risk Management framework, and the EU AI Act. The tool will provide an open access, simplified baseline of requirements for responsible and trustworthy AI development and deployment.

   As of 20th January 2025, the AIME tool design is open for review via public consultation. We intend to make an online version of the tool publicly available in the summer of 2025.

ii. AIME will be a voluntary initiative at first. The onus will be on self-assessment users to identify and address limited areas of governance – including practices with human rights implications – through engaging thoroughly with the tool, deliberating upon its recommendations, and formulating their own plans to improve compliance and redress mechanisms within their organisation if required.

Following launch of the voluntary tool, we are looking to embed AIME into government procurement frameworks to create a baseline requirement for government suppliers of AI products and services. To achieve a rigorous baseline, more formal mechanisms for demonstrating performance may need to be adopted, such as providing evidence against criteria or successful completion of relevant certification programmes.

iii. AIME asks users to respond to a series of questions about their organisational AI management system using multiple choice options. Current questions that relate directly to corporate responsibilities surrounding human rights include:

- Do you develop or use AI systems that directly impact individuals?
- Do you have clear definitions of fairness with respect to these AI systems?
- Do you have mechanisms for detecting or identifying unfair outcomes or processes with respect to these AI systems and your definitions of fairness?
- Where appropriate, do you have an impact assessment process for identifying how your AI systems might impact the legal position or life opportunities if individuals?
- If you procure AIaaS or pretrained AI systems from third party providers, do you conduct appropriate due diligence on the data used to train or develop these systems to mitigate against foreseeable harmful or unfair bias?
- Do you have reporting mechanisms for all employees, users and external third parties to report concerns or system failures?

iv. AIME does not provide sector specific measures or guidance.

Outside of Government, legal services regulators have taken steps support the safe implementation and adoption of AI. For example, The Legal Services Board (LSB) – an oversight regulator – published new statutory guidance (here) in April 2024 which sets out three outcomes that legal sector regulators are expected to pursue when developing their own approaches to technology and innovation, including AI. The objectives were to address barriers that consumers, technology providers, and legal services providers currently face, as well as helping to promote the use of technology and innovation to increase access to justice.

The Solicitors Regulatory Authority (SRA), who are the regulatory body for solicitors in England and Wales, were awarded a grant in the latest round of the Regulators Pioneer Fund (please find the article here). The money funds a project to explore ways to increase the use of technology-enabled dispute resolution to help individuals and businesses resolve legal issues, without the need to go to court. This includes thinking about the role AI could play in helping to identify legal needs and problems. The project concludes in February 2025.

UKRAINE

In 2020-2021, Ukraine adopted the **Concept for the Development of Artificial Intelligence in Ukraine** and **the Action Plan for its Implementation** (link). The Concept identified nine priority areas for implementing state policy for the AI industry's development: education, science, economy, cybersecurity, defence, information security, public administration, legal regulation and ethics, and justice.

In April 2024, the Cabinet of Ministers of Ukraine approved **the Concept of the State Targeted Scientific and Technical Program for the Use of Artificial Intelligence Technologies in Priority Economic Sectors until 2026** (link). This program aims to define the directions and objectives for developing artificial intelligence technologies and introduce mechanisms for state support, which will enhance Ukraine's economic potential and strengthen its position on the global market. AI legal alignment with the EU norms and AI sector development are among the top priorities for the Government of Ukraine.

Besides, the **WINWIN 2030 Strategy** (link) defines the key areas of our technological development within the public and international sectors. AI is one of the 7 main areas of the innovation strategy, which describes priority industries that need to be developed in Ukraine.
Roadmap for the Regulation of Artificial Intelligence in Ukraine (link) proposes and describes Ukraine's bottom-up approach to regulating AI, which should allow Ukrainian AI companies to be internationally competitive, attract investments, and provide a safe digital environment for citizens.

Based on the Roadmap **the AI White Paper** (link), a policy and strategic document, was developed. It clearly informs the industry that legally binding legislation will be introduced gradually in two stages and encourages proactive action.

Ukraine also introduces soft law tools to adhere to ethical standards and promote public trust in AI interactions. These are primarily **general and sectoral recommendations** (already adopted on Media, Intellectual Property, Schools, for Journalists). An example of sectoral recommendations — Recommendations on the Responsible Use of Artificial Intelligence in the Media — can be found here.

In addition to recommendations, Ukraine adopted another tool — a set of voluntary commitments in **a voluntary code of conduct** — to expand and strengthen the legally non-binding role of general and sectoral recommendations.
We also work to pilot **HUDERIA** (Human Rights, Democracy, and the Rule of Law Impact Assessment for AI Systems) – a methodology to assess the impact of AI technologies on human rights and democratic values.
Ukraine is a proactive participant in the international AI governance ecosystem and follow best international standards in AI regulations. One of the goals of AI policy in Ukraine is to gradually and organically integrate the principles of the **EU AI Act.** After giving businesses time and tools to prepare and build the state's capacity to regulate AI, it is planned to develop and adopt a law analogous to the EU AI Act.

Sandbox is a controlled environment within which participating companies can develop and test their AI applications for compliance with future legislation (the analogous law to the AI Act) under the supervision of the state. The state supports participants in the development of their products so that they comply with the AI Act. The purpose of the regulatory sandbox is to provide companies with a practical tool to prepare for future national legislation and simplify entry into the EU market in the near future. Will be launched by the end of the 2024 year.

At the same time, we actively monitor the emergence of new tools and initiatives on responsible AI at the international level, in other countries, as well as at the level of public sector and industry initiatives. Ukraine is following **the OECD and UNESCO recommendations on AI.**

Ukraine signed **the Bletchley Declaration** at the AI Safety Summit 2023, which supported the idea of creating a framework to ensure that AI technologies are developed and used responsibly and safely around the world.

Finally, Ukraine is developing a new **National AI Strategy** to provide comprehensive policy goals for implementing AI in critical sectors, such as defence, education, reconstruction, public services, economy, and innovations.