Comité d'experts sur les droits des usagers d'internet (MSI-NET)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

MSI-NET (2016)09
10 octobre 2016

2e réunion, 29-30 septembre 2016, 9 h 30-17 h 30
(Strasbourg, Palais de l'Europe, salle 7)

Rapport de réunion

1. M. Jan Kleijssen, directeur de la Direction de la société de l'information et de la lutte contre la criminalité, ouvre la réunion et souhaite la bienvenue aux membres du MSI-NET et aux participants. Donnant au MSI-NET des informations se rapportant à ses travaux, il évoque la conférence sur « la liberté d'internet : un facteur constant de la sécurité démocratique en Europe » organisée le 9 septembre 2016 à Strasbourg. Il mentionne les travaux d'autres organes du Conseil de l'Europe relatifs aux intermédiaires de l'internet, comme le groupe sur les preuves dans le nuage de la Convention sur la cybercriminalité, et la nécessité d'une bonne coordination avec d'autres entités est soulignée. Il informe le MSI-NET de l'initiative du Conseil de l'Europe de créer une plateforme pour favoriser le dialogue entre les Etats membres et les entreprises du secteur d'internet afin d'améliorer le respect des droits de l'homme, de la démocratie et de l'état de droit en ligne. Pour finir, il souligne l'utilité d'examiner des questions comme les rôles et les responsabilités des intermédiaires de l'internet, les répercussions des algorithmes et des autres développements connexes, dont l'intelligence artificielle, sur les droits de l'homme.

2. Le Secrétariat donne au MSI-NET des informations sur la 10e réunion du CDMSI (comité directeur sur les médias et la société de l'information) qui a eu lieu du 28 juin au 1er juillet 2016.

3. L'ordre du jour (annexe 1) est adopté sans modifications. La liste des participants est reproduite à l'annexe 2. La répartition hommes-femmes des 39 participants est la suivante : 20 femmes (51 %) et 19 hommes (49 %).

Conclusions et décisions

4. Pour ce qui est du premier résultat attendu, à savoir un *projet de recommandation du Comité des Ministres sur les intermédiaires de l'internet*, le MSI-NET examine la première version du document présenté par le rapporteur, M. Matthias Kettemann (annexe 3). Il décide de retenir une large définition fondée sur les fonctions des intermédiaires de l'internet. Il reconnaît la nécessité impérative de donner aux Etats des orientations sur leur interaction et sur la réglementation des intermédiaires de l'internet ; il pourrait y contribuer sous l'angle des droits de l'homme et de l'état de droit. Les obligations négatives et positives

des Etats en ce sens pourraient être précisées. La tendance actuelle à s'écarter du régime de responsabilité limitée des intermédiaires de l'internet et la nécessité de voir dans ce régime un moyen de protéger les droits de l'homme et la libre circulation des informations sont aussi reconnues. Le comité décide aussi de développer la partie consacrée à l'amélioration de la protection des droits de l'homme des usagers dans leurs rapports avec les intermédiaires de l'internet, en particulier en soulignant les garanties d'une procédure régulière. Un certain nombre d'observations, de commentaires et de propositions de changement sur le projet de recommandation sont examinés pendant la réunion ; ils apparaîtront dans le projet révisé de recommandation du rapporteur.

5. En ce qui concerne le *rapport sur les dimensions des droits de l'homme dans l'application des algorithmes*, le MSI-NET examine la première version du document présenté par le rapporteur, M. Ben Wagner (annexe 4). L'utilité de ce rapport pour sensibiliser au sujet et la nécessité d'expliquer spécifiquement et clairement les répercussions des algorithmes sur les droits de l'homme sont reconnues. La discussion sur la définition des algorithmes met en évidence la difficulté de saisir un environnement numérique qui évolue rapidement. Les études de cas utilisées pour illustrer ces répercussions sont longuement examinées en vue de les développer et de recenser les droits de l'homme concrets qui sont en jeu. Un certain nombre d'observations, de commentaires et de propositions de changement sont examinés ; ils apparaîtront dans le projet révisé de recommandation du rapporteur.

6. EuroISPA dit ce qu'elle pense de la mise à jour des lignes directrices visant à aider les fournisseurs de services internet, rédigées en 2008 en coopération avec le Conseil de l'Europe. L'association fait observer qu'elle a suivi les débats du MSI-NET et qu'elle optera pour une actualisation des lignes directrices parallèlement au projet de recommandation.

6. Le MSI-NET discute de la participation à des manifestations visant à assurer le concours et la participation de multiples parties prenantes à ses activités, notamment dans le contexte du FGI. Le président présentera les travaux du MSI-NET et demande au Secrétariat de proposer des tours de parole lors des ateliers du FGI et des manifestations auxquelles il pourrait participer.

Questions diverses

7. Les membres du MSI-NET s'accordent sur la nécessité d'organiser une consultation avec d'autres comités directeurs et conventionnels compétents du Conseil de l'Europe ainsi qu'avec d'autres parties prenantes avant d'établir la version définitive du projet de recommandation sur les intermédiaires de l'internet et du projet de rapport sur les algorithmes. Il est demandé au Secrétariat de faire des propositions de dates à cette fin en tenant compte en particulier des réunions du CDMSI en 2017.

8. Le MSI-NET convient provisoirement d'organiser sa prochaine réunion les 27 et 28 mars 2017 à Strasbourg.

9. Le Secrétariat élaborera un projet de rapport de réunion qui sera soumis à l'examen de la présidence et de la vice-présidence. Il enverra ensuite le projet de rapport au MSI-NET qui disposera d'un délai de cinq jours ouvrables pour formuler des observations. En l'absence d'observations, le rapport sera considéré comme définitif et transmis au CDMSI pour information. L'état d'avancement des travaux du MSI-NET sera indiqué dans les projets de documents et dans les rapports de réunion du comité. Il est donc jugé inutile d'élaborer des rapports de réunion abrégés.

ANNEXE I

ORDRE DU JOUR ANNOTE[1]

1. Ouverture de la réunion
par M. Jan KLEIJSSEN, Directeur, Direction de la Société de l'information et de la lutte contre la criminalité

2. Adoption de l'ordre du jour

3. Information du Secrétariat
Informations sur les travaux normatifs et autres activités du Conseil de l'Europe d'importance pour le MSI-NET, notamment la 10ème réunion plénière du CDMSI (Comité Directeur sur les Médias et la Société de l'Information), 28 juin – 1er juillet 2016.

4. Discussion du projet de recommandation du Comité des Ministres sur les intermédiaires internet
[MANDAT MSI-NET] *(doc MSI-NET(2016)05)*
Les membres du MSI-NET seront invités à examiner et à discuter la première version du projet de recommandation préparé par le rapporteur.

5. Discussion du projet de rapport sur les dimensions des droits de l'homme dans l'application des d algorithmes
[MANDAT MSI-NET] *(doc MSI-NET (2016)06)*
Les membres du MSI-NET seront invités à examiner et à discuter la première version du projet de rapport préparé par le rapporteur.

6. Lignes directrices visant à aider les fournisseurs de services Internet
Une présentation sera faite par le représentant d'EuroISPA. Les membres du MSI-NET seront invités à discuter de la possible mise à jour des lignes directrices.
Lignes directrices visant à aider les fournisseurs de services Internet

7. Participation du MSI-NET à d'autres activités
Les membres du MSI-NET seront invités à partager toute information concernant leur participation passée et future à d'autres activités pertinentes au travail du comité

8. Dates de la prochaine réunion

9. Autres points

[1] Tel que reproduit sous le document MSI-NET(2016)08

ANNEXE 2

LISTE DES PARTICIPANTS

COMMITTEE MEMBERS	MEMBRES DU COMITE
Mr Bertrand de la CHAPELLE – Co-founder and Director of the Internet & Jurisdiction Project, France	M. Bertrand de la CHAPELLE – Co-fondateur et Directeur du Projet Internet & Jurisdiction, France
Ms Julia HÖRNLE – Professor of Internet Law, Queen Mary University of London apologised	*Mme Julia HÖRNLE – Professeur des lois dans le domaine d'Internet, Queen Mary University of London excusée*
Ms Tanja KERŠEVAN-SMOKVINA – Principal Advisor to Director General, Agency for Communication Networks and Services, Slovenia	Mme Tanja KERŠEVAN-SMOKVINA - Conseillère principale auprès du directeur général - Agence pour les réseaux et services de communication – Slovénie
Mr Matthias KETTEMANN – Postdoc Fellow, Cluster of Excellence "Normative Orders" University of Frankfurt/Main (Germany) Austria (Rapporteur Recommendation)	M. Matthias KETTEMANN – Postdoc Fellow, Cluster of Excellence "Normative Orders" Université de Francfort-sur-le-Main (Allemagne) Autriche (Rapporteur Recommandation)
Ms Sabine MAASS – Head of Division 'Legal framework for digital services, media industry', Federal Ministry for Economic Affairs and Energy – Germany (apologized)	*Mme Sabine MAASS – Chef de la division «Cadre juridique pour les services numériques, l'industrie des médias», Ministère Fédéral de l'Economie et de l'Energie – Allemagne* (*excusée)*
Mr Arseny NEDYAK – Deputy Director, Department of Media State Policy, Ministry of Telecommunication, Russian Federation	M. Arseny NEDYAK – Directeur adjoint, Service des politiques nationales des médias, Ministère de la télécommunication – Fédération de Russie
Mr **Pēteris** PODVINSKIS – Ministry of Foreign Affairs, International Organisations Directorate, Department for Public Policy related to Internet – Latvia	M. **Pēteris** PODVINSKIS – Ministère des affaires étrangères, Direction Organisations Internationales, Service des Politiques publiques dans le domaine de l'Internet – Lettonie
Mr Thomas SCHNEIDER – Deputy Director of International Affairs, International Information Society Coordinator, Federal Department of the Environment, Transport, Energy and Communication DETEC, Federal Office of Communications (OFCOM), Switzerland	M. Thomas SCHNEIDER – Directeur adjoint des affaires internationales, Coordinateur de la société d'information internationale, Service fédéral de l'environnement, transport, énergie et communication DETEC, Office fédéral des communications (OFCOM) – Suisse
Mr Wolfgang SCHULZ – Professor, Faculty of Law, University of Hamburg / Hans-Bredow-Institut (Chair)	M. Wolfgang SCHULZ – Professeur, Faculté de droit, Université de Hambourg / Institut de Hans-Bredow (président)

Ms Sophie STALLA-BOURDILLON – Associate Professor in Information Technology / Intellectual Property Law, Director of ILAWS, Southampton Law School
University of Southampton

Ms Karmen TURK – Trinity Tallinn – Estonia
(Vice-Chair)

Mr Dirk VOORHOOF – Lecturer European Media Law, UCPH (Copenhagen University) / Professor at Ghent University, member of the Centre for Media Pluralism and Press Freedom (CMPF) Scientific Committee

Mr Benjamin WAGNER – Director of the Centre for Internet & Human Rights, European University Viadrina, Frankfurt/Oder (Rapporteur Report HR dimensions on Algorithms)

Mme Sophie STALLA-BOURDILLON – Professeur agrégée en technologie d'information / droit de la propriété intellectuelle, Directrice de ILAWS, Faculté de droit de Southampton
Université de Southampton

Mme Karmen TURK – Trinity Tallinn – Estonie
(vice-présidente)

M. Dirk VOORHOOF – M. Dirk VOORHOOF – Professeur de droit européen des media, UCPH (Université de Copenhague) / Professeur à l'université de Gand, membre du comité scientifique du Centre pour le pluralisme des médias et la liberté de la presse (CMPF)

M. Benjamin WAGNER – Directeur du Centre pour l'Internet & les droits de l'Homme, Université européenne Viadrina, Francfort/Oder (Rapporteur rapport aspect des DH dans le domaine des algorithmes)

COUNCIL OF EUROPE MEMBER STATES

AZERBAIJAN

Mr. Bakhtiyar MAMMADOV, Chief advisor, Ministry of Communications and High Technologies of the Republic of Azerbaijan

GERMANY

Ms Dörte NIELANDT, Deputy Head of Division „Legal framework for digital services, media industry" - Federal Ministry for Economic Affairs and Energy – Germany

ITALY

Ms Francesca PELLICANO, Autorità per le Garanzie nelle Comunicazioni, Roma / Napoli

POLAND

Ms Marta KACZMARSKA, Deputy to the Permanent Representative, Permanent Representation of Poland to the Council of Europe, Strasbourg

SPAIN

Ms María REYES FERNÁNDEZ, Legal Advisor, Directorate on Information Society Services, Secretary of State for Telecommunications and Information Society - Spain

ETATS MEMBRES DU CONSEIL DE L'EUROPE

AZERBAÏDJAN

M. Bakhtiyar MAMMADOV, Conseiller principal, Ministère de la communication et des hautes technologies de la République d'Azerbaïdjan

ALLEMAGNE

Mme Dörte NIELANDT, adjointe au chef de division „Cadre juridique des services numériques et l'industrie des medias"- Ministère Fédéral de l'Economie et de l'Energie – Allemagne

ITALIE

Mme Francesca PELLICANO, Autorità per le Garanzie nelle Comunicazioni, Roma / Napoli

POLOGNE

Mme Marta KACZMARSKA, Adjointe au Représentant Permanent, représentation permanente de la Pologne auprès du Conseil de l'Europe, Strasbourg

ESPAGNE

Ms María REYES FERNÁNDEZ, Conseillère juridique, Direction des services de la société de l'information, Secrétariat d'Etat aux Télécommunications et à la Société de l'Information - Espagne

SWITZERLAND

Mr Jorge CANCIO, International Relations, Federal Department of the Environment, Transport, Energy and Communication DETEC, Federal Office of Communications (OFCOM) – Switzerland apologised

SUISSE

M. Jorge CANCIO, Relations Internationales, Service fédéral de l'environnement, transport, énergie et communication DETEC, Office fédéral des communications (OFCOM) – Suisse
Excusé

TURKEY

Mr. Erhan BAL, Radio and Television Supreme Council (RTÜK)

TURQUIE

M. Erhan BAL, Conseil supérieur de la Radio et de la Télévision (RTÜK)

PARTICIPANTS

EUROPEAN COMMISSION - DG CONNECT

Ms Irene ROCHE LAGUNA, Legal officer, DG for Communications Networks, Content & Technology

EUROPEAN AUDIOVISUAL OBSERVATORY

Department for Legal Information

Ms Maja CAPPELLO, Head of Department

OSCE

Office of the Representative on Freedom of the Media

Mr Frane MAROEVIC, Director (apologized)

MEXICO

Mr Diego SANDOVAL PIMENTEL, Deputy to the Permanent Observer of Mexico to the Council of Europe

REPRESENTATIVES OF CIVIL SOCIETY, ACADEMIC COMMUNITIES AND THE PRIVATE SECTOR

Ms Christina ANGELOPOULOS, Information Law and Policy Centre, Institute of Advanced Legal Studies, School of Advanced Study, University of London (UK)

Mr Pierre François DOCQUIR, ARTICLE 19, Defending freedom of expression and information (London)

Mr Martin HUSOVEC, Assistant Professor, Tilburg Institute for Law, Technology and Society (TILT, University of Tilburg, Netherlands)

Ms Aleksandra KUCZERAWY, Legal Researcher, Centre for IT & IP Law – iMinds, Univeristy Leuven, Belgium

PARTICIPANTS

COMMISSION EUROPEENNE - DG CONNECT

Mme Irene ROCHE LAGUNA, juriste, DG des réseaux de communication, du contenu et des technologies

OBSERVATOIRE EUROPEEN DE L'AUDIOVISUEL

Service des Informations juridiques

Mme Maja CAPPELLO, Chef de service

OSCE

Bureau du Représentant pour la liberté des médias

M. Frane MAROEVIC, Directeur (excusé)

MEXIQUE

M. Diego SANDOVAL PIMENTEL, Adjoint à l'Observateur Permanent du Mexique auprès du Conseil de l'Europe

REPRESENTANTS DE LA SOCIETE CIVILE, DU MILIEU UNIVERSITAIRE ET DU SECTEUR PRIVE

Mme Christina ANGELOPOULOS, Information Law and Policy Centre, Institute of Advanced Legal Studies, School of Advanced Study, University of London (Université de Londres)

M. Pierre François DOCQUIR, ARTICLE 19, Defending freedom of expression and information (Londres)

M. Martin HUSOVEC, Assistant Professor, Tilburg Institute for Law, Technology and Society (TILT, Université de Tilburg, Pays-Bas)

Mme Aleksandra KUCZERAWY, chercheuse en droit, Centre de Droit des TI & PI, Université de Louvain, Belgique

Mr Joe McNAMEE, Executive director, European Digital Rights (EDRi), Brussels, Belgium	M. Joe McNAMEE, Directeur Exécutif, European Digital Rights (EDRi), Bruxelles, Belgique
Ms Aibhinn KELLEHER, FACEBOOK Ireland Ltd (Dublin)	Mme Aibhinn KELLEHER, FACEBOOK Ireland Ltd (Dublin)
Mr Michael ROTERT, Honorary Spokesman, EuroISPA (European Internet Service Provider Association)	M. Michael ROTERT, porte-parole honoraire, EuroISPA (European Internet Service Provider Association)
Ms Karen WHITE, TWITTER (apologised)	Mme Karen WHITE, TWITTER (excusée)
Mr Marco PANCINI, GOOGLE (apologised)	M. Marco PANCINI, GOOGLE (excusé)
OBSERVERS	**OBSERVATEURS**
EBU – European Broadcasting Union apologised	UER - Union Européenne de Radio-télévision excusée
MOROCCO	MAROC
Ms Chanaz el AKRICHI, Head of Cooperation division, Ministry of Communication	Mme Chanaz el AKRICHI, Chef de la division de la Coopération, Ministère de la Communication
Ms Meriem KHATOURI, Director for Media Studies and Development, Ministry of Communication	Mme Meriem KHATOURI, Directrice des études et du développement des médias, Ministère de la Communication
COUNCIL OF EUROPE	**CONSEIL DE L'EUROPE**
DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW	DIRECTION GÉNÉRALE DROITS DE L'HOMME ET ETAT DE DROIT
Mr Jan KLEIJSSEN, Director, Directorate of Information Society and Action against Crime	M. Jan KLEIJSSEN, Directeur, Direction de la Société de l'information et de la lutte contre la criminalité
Mr Patrick PENNINCKX, Head of Information Society Department	M. Patrick PENNINCKX, chef du service de la Société de l'information
Ms. Silvia GRUNDMANN, Head of Media and Internet Division, Information Society Department	Mme Silvia GRUNDMANN, chef de la division médias et internet, service de la Société de l'information
Mr Alexandru FRUNZA, Project Officer, Cybercrime Division, Information Society Department	M. Alexandru FRUNZA, Chargé de Projet, division de la Cybercriminalité, service de la Société de l'information
Mr Octavian SOFRANSKY, Data Protection Unit Information Society Department	M. Octavian SOFRANSKY, Unité Protection des Données, service de la Société de l'information
Ms Elvana THAÇI, Head of Standard Setting Unit, MSI-NET Secretariat, Media and Internet Division, Information Society Department	Mme Elvana THAÇI, Chef de l'unité normative, Secrétariat MSI-NET, division médias et internet, service de la société de l'information
Ms Charlotte ALTENHÖNER-DION, Administrator, MSI-NET Secretariat, Media and Internet Division, Information Society Department	Mme Charlotte ALTENHÖNER-DION, administratrice, Secrétariat MSI-NET division médias et internet, service de la société de l'information

Ms Ana GASCÓN MARCÉN, Administrator, MSI-NET Secretariat Media and Internet Division, Information Society Department	Mme Ana GASCÓN MARCÉN, Administratrice, Secrétariat MSI-NET division médias et internet, service de la Société de l'information
Ms Małgorzata PEĶ, Project Officer, Media and Internet Division, Information Society Department	Mme Małgorzata PEĶ, Chargée de projet, division médias et internet, service de la Société de l'information
Ms Elisabeth MAETZ, Assistant, Media and Internet Division Information Society Department	Mme Elisabeth MAETZ, Assistante, division médias et internet, service de la Société de l'information

INTERPRETERS / INTERPRETES

Clarissa WORSDALE, Martine KARALY, Isabelle MARCHINI

ANNEXE 3[2]

Projet de Recommendation CM/Rec(2017x)xx du Comité des Ministres aux Etats membres sur les intermédiaires Internet

Premier Projet (13 septembre)
Présenté lors de la deuxième réunion (29-30 septembre 2016)

Rapporteur : Matthias C. Kettemann

1. Toute personne jouit du droit d'accès à internet, qui est inhérent au droit à la liberté d'expression protégé par l'article 10 de la Convention européenne des droits de l'homme (STE n° 5, ci-après « la Convention »). Les Etats membres du Conseil de l'Europe sont tenus de garantir à toute personne relevant de leur juridiction les droits de l'homme et les libertés fondamentales sur internet.

2. Les intermédiaires internet jouent un rôle de premier plan en fournissant un accès à l'internet et à son contenu à des milliards d'usagers et sont structurellement essentiels à tous les flux de données en ligne. Ils gèrent les contenus en ligne et en contrôlent l'accès. Les conditions de fait et de droit qui régissent la fourniture d'accès à internet, la recherche, la communication et la réception d'informations, ainsi que l'agrégation et la gestion des données par les intermédiaires internet, sont définies par un ensemble complexe de lois nationales, de règles européennes et internationales, de conditions de service, d'instruments de droit souple et de codes. Conformément à leurs obligations négatives et positives relatives aux droits de l'homme, les Etats membres doivent établir un cadre juridique qui permet aux intermédiaires internet de jouer ce rôle essentiel sans violer les droits de l'homme.

3. Les Etats membres sont confrontés à la nécessité de concilier des objectifs contradictoires et de rechercher un équilibre entre les droits concurrents, dans un contexte de plus en plus international compliqué par les caractéristiques de la technologie internet ainsi que par les multiples fonctions et la nature diverse des intermédiaires internet.

4. Par conséquent, le Comité des Ministres, soucieux de guider les Etats membres dans l'élaboration et l'application de la législation sur les intermédiaires internet, en vertu de l'article 15.b du Statut du Conseil de l'Europe, recommande aux Etats membres :

- de veiller à s'acquitter de leur obligation positive et négative de garantir les droits de l'homme de toute personne relevant de leur juridiction, conformément aux articles 8 et 10 de la Convention, lorsqu'ils réglementent les activités des intermédiaires internet ;

- de prendre toutes les mesures nécessaires, en coopération avec tous les acteurs concernés, pour que les intermédiaires internet puissent remplir leur rôle et développer leur potentiel dans la société de l'information sans violer les droits de l'homme ;

[2] telle que reproduit sous document MSI-NET(2016)05 du 13 septembre 2016

- de remplir, en ligne et hors ligne, l'obligation primordiale qui leur incombe de protéger les droits de l'homme et l'état de droit, y compris par des garanties procédurales et des voies de recours effectives en cas de violation des droits ;

- ce faisant, d'adopter des cadres d'action nationaux et de contribuer aux cadres d'action régionaux et internationaux, en tenant dûment compte des lignes directrices sur les intermédiaires internet exposées dans l'annexe à la présente recommandation ;

- de promouvoir ces lignes directrices dans d'autres enceintes internationales et régionales qui traitent des intermédiaires internet.

Annexe à la recommandation : lignes directrices sur les intermédiaires internet

1. Principes généraux

1.1. Conformément à la Recommandation CM/Rec(2016)3 du Comité des Ministres aux Etats membres sur les droits de l'homme et les entreprises, dans le cadre de leur juridiction, les Etats ont l'obligation primordiale de respecter, de protéger et de réaliser tous les droits et libertés garantis à toute personne par la Convention européenne des droits de l'homme, aussi bien en ligne que hors ligne.

1.2. Les Etats sont tenus d'établir un cadre juridique, fondé sur la Convention et conforme aux principes bien établis des droits de l'homme, de la démocratie et de l'état de droit, qui favorise un environnement en ligne propice au débat public.

1.3. Les organes spécialisés de la société, tels que les intermédiaires internet, doivent se conformer à toutes les lois applicables et respecter les droits de l'homme (« responsabilité des entreprises de respecter les droits de l'homme »). Des voies de recours appropriées, aisément accessibles et effectives devront compenser les manquements des Etats et des organes spécialisés à leurs obligations en matière de droits de l'homme.

1.4. Toute personne a le droit de participer à la société de l'information. Le droit d'accès à internet est inhérent au droit d'accéder à l'information et à la communication, qui est protégé par la Convention. Dès lors, les Etats membres sont tenus de garantir à leurs citoyens l'accès à internet (Yildirim, 2012, paragraphe 31). Pour améliorer l'accès du public à l'actualité et à d'autres informations, il est indispensable de protéger l'accessibilité d'internet ainsi que sa capacité à conserver et à diffuser de grandes quantités de données (Times Newspapers Ltd., 2009, paragraphe 27).

1.5. La protection des intermédiaires internet complète le droit d'accès. Les intermédiaires internet jouent un rôle central en assurant l'accès au contenu d'internet, en tant que fournisseurs d'accès et en tant qu'hébergeurs de contenu. Ainsi, ils constituent des sources précieuses d'informations souvent spécifiques et ont joué un rôle déterminant dans l'émergence du journalisme citoyen (Cengiz, 2015).

1.6. Si l'exercice effectif des droits prévus à l'article 10 exige de mettre en œuvre des mesures de protection positives, y compris entre les individus ou entre les individus et les intermédiaires internet, il incombe aux Etats membres d'adopter une législation appropriée au niveau national.

1.7. Lorsqu'ils réglementent les intermédiaires internet, les Etats membres doivent ménager un juste équilibre entre l'intérêt général de la société, les intérêts de l'individu et l'intérêt de l'intermédiaire (Özgür Gündem, 2000, paragraphe 43).

1.8. Afin de garantir le droit d'accès à internet et la protection des intermédiaires internet, les Etats prennent des mesures positives et, au besoin, réglementent les intermédiaires internet. Ces derniers jouent un rôle fondamental dans l'économie numérique, et toute réglementation les concernant doit faire en sorte qu'ils puissent continuer à offrir et à développer des services innovants, tout en garantissant que tout nouveau service soit conforme aux lois en vigueur et respecte les droits de l'homme.

1.9. Les Etats membres veillent à ce que la réglementation des intermédiaires internet soit, dans la mesure du possible, flexible évolutive et propice à l'innovation, et assure un équilibre approprié en cas d'interprétation conflictuelle des droits de l'homme.

1.10. Les Etats membres ne délèguent pas des mesures de censure à des organismes privés, ne privatisent pas les services chargés de l'application des lois, ni ne confèrent aux intermédiaires des fonctions quasi-judiciaires sans les garanties appropriées. Les intermédiaires internet devraient décliner les invitations à exercer de telles fonctions.

1.11. Toute restriction du droit à la liberté d'expression des intermédiaires doit être prévue par la loi, poursuivre l'un des buts légitimes énumérés de façon exhaustive à l'article 10, paragraphe 2, de la Convention, et être nécessaire et proportionnée dans une société démocratique.

1.12. Pour que la liberté d'expression s'exerce sur les réseaux et les plateformes des intermédiaires internet en accord avec une conception centrée sur les droits de l'homme, il convient que les conditions de service soient transparentes et interprétées conformément aux normes internationales relatives aux droits de l'homme, que ces conditions soient appliquées et mises en œuvre de manière cohérente et proportionnée, et que les usagers aient accès à un mécanisme de recours. En outre, les sociétés privées devraient s'abstenir d'imposer des restrictions à la liberté d'expression allant au-delà des exigences de la loi.

2. Protection du rôle de facilitation des intermédiaires internet

2.1. Les Etats membres veillent à ce que la responsabilité des intermédiaires internet soit délimitée conformément, en particulier, aux articles 8, 10 et 13 de la Convention.

2.2. Pour réglementer la responsabilité des intermédiaires internet, les Etats membres adoptent une approche fondée sur les activités afin que les acteurs d'internet qui exercent un vaste éventail d'activités puissent bénéficier d'exonérations de responsabilité (civile et pénale) dans les cas où 1) ils agissent en tant que canaux d'expression pour des tiers dans le cadre d'une activité spécifique (fonction de recherche, section de commentaires générés par les usagers, par exemple) et 2) ils mettent en œuvre de bonnes pratiques de transparence lorsqu'ils traitent les contenus de tiers.

2.3. Les Etats membres encouragent le développement de bonnes pratiques de transparence pour le traitement des contenus de tiers (par l'adoption de codes de conduite par exemple).

2.4. Les Etats membres ne demandent pas aux intermédiaires internet d'évaluer la légalité d'un contenu de tiers. Ils peuvent apprécier si le contenu enfreint ou non leurs conditions de service, mais doivent procéder de manière non discriminatoire et veiller à ce que les conséquences de cette appréciation soient clairement communiquées, de même que les possibilités de recours, et qu'elles ne constituent pas une discrimination ni d'autres violations des droits de l'homme.

2.5. Les intermédiaires internet sont tenus de réagir rapidement face à un contenu illicite uniquement si une procédure claire, prévisible et proportionnée a été mise en place. La nature de cette procédure devrait dépendre de son incidence sur le droit au respect de la vie privée et le principe de confidentialité des communications, prévus à l'article 8, et sur la liberté d'expression des usagers d'internet, protégée par l'article 10 de la Convention.

2.6. Différentes procédures devraient être suivies lorsque la réclamation relative à un contenu concerne un différend de caractère privé (droits d'auteur, pour lesquels un système de notification serait préférable, par exemple) et lorsque le contenu en question est criminel (incitation à la violence, par exemple).

2.7. Les Etats membres demandent aux intermédiaires internet opérant au niveau de l'application de retirer le contenu illicite uniquement lorsqu'ils en ont connaissance ou s'ils ont été informés de la présence/transmission de contenus manifestement illicites dans leurs systèmes.

2.8. Les fournisseurs d'accès à internet sont tenus de bloquer l'accès à un contenu illégal uniquement en conséquence d'une ordonnance judiciaire. Lorsqu'ils s'opposent à des ordonnances de blocage, les frais de précontentieux et les frais de justice ne sont pas à leur charge. Les intermédiaires internet intervenant au niveau de l'application n'assument pas les frais de précontentieux et les frais de justice lorsque le contenu en question n'est pas jugé manifestement illicite.

2.9. Les Etats membres mettent en place des procédures de notification et de contre-notification, que les intermédiaires internet au niveau de l'application doivent suivre lorsqu'ils réagissent à un contenu illicite et qui doivent effectivement impliquer à la fois les émetteurs et les destinataires du contenu afin de permettre l'exercice du droit à un recours effectif protégé par l'article 13 de la Convention.

2.10. En vue d'émettre des notifications à l'attention des intermédiaires internet intervenant au niveau de l'application, les Etats membres envisagent de mettre en place au sein de leurs systèmes judiciaires des procédures de notification et de contre-notification largement accessibles et rapides, plus respectueuses des droits de l'homme que les procédures de notification et de contre-notification (purement) privées

2.11. Les Etats membres favorisent le développement de bonnes pratiques permettant de reconnaître rapidement des contenus manifestement illicites qui devraient reposer sur des procédures de notification et de contre-notification par l'adoption d'instruments sectoriels comme des codes de conduite.

2.12. Les intermédiaires internet ne sont pas tenus (après la réception de notifications ou l'émission d'ordonnances judiciaires) de surveiller systématiquement leurs systèmes afin de prévenir toute activité illicite, en particulier lorsque la surveillance systématique de contenus de tiers suppose la mise en œuvre de mesures intrusives sur le plan de la vie privée, lorsque la surveillance systématique de contenus de tiers peut entraîner des mesures de surblocage, ou lorsque la surveillance systématique de contenus de tiers impose une trop lourde charge financière aux intermédiaires internet.

2.13. Les Etats membres n'encouragent pas les intermédiaires internet à surveiller volontairement leurs systèmes de manière systématique pour éviter toute activité illicite, si la surveillance systématique de contenus de tiers suppose d'appliquer des mesures intrusives sur le plan de la vie privée et/ou de surblocage.

2.14. Pour déterminer si des mesures sont intrusives sur le plan de la vie privée, il faut tenir compte du rôle joué par les intermédiaires internet dans le processus de transmission des communications et des effets du principe de confidentialité des communications prévu par l'article 8 de la Convention.

2.15. Les Etats membres envisagent l'adoption de règles sectorielles relatives à la répartition des coûts de mise en œuvre du blocage ou du retrait afin que les intermédiaires internet puissent en demander le remboursement à certaines catégories de victimes (les titulaires de droits de propriété intellectuelle par exemple), dans la mesure où le droit à un recours effectif, prévu à l'article 13 de la Convention, n'est pas compromis.

3. Limites à la réglementation des intermédiaires

3.1. Les Etats sont tenus de combattre la violence et les autres activités criminelles ou illicites en ligne. A cette fin, ils peuvent être amenés à imposer aux intermédiaires l'obligation de retirer des contenus, de communiquer des informations sur les usagers ou de suspendre l'accès dont bénéficiaient des usagers ou l'accès à des noms de domaines.

3.2. Etant donné l'importance du droit d'accès à internet et de la liberté d'expression, toute restriction concernant les intermédiaires qui a une incidence sur ces droits doit être prévue par la loi, poursuivre l'un des buts légitimes énumérés de façon exhaustive à l'article 10, paragraphe 2, de la Convention, et être nécessaire et proportionnée dans une société démocratique.

3.3. Toute loi ou réglementation régissant la responsabilité des intermédiaires doit être accessible et suffisamment précise pour qu'ils puissent prévoir les conséquences de leur comportement. De plus, afin de satisfaire aux exigences d'accessibilité et de prévisibilité, la loi doit offrir une protection juridique contre l'arbitraire et définir des garanties procédurales appropriées afin de protéger de manière effective les droits énoncés par la Convention, notamment le droit à la liberté d'expression. Cette protection ne se limite pas aux ingérences des pouvoirs publics dans l'exercice du droit à la liberté d'expression. Il incombe en outre aux Etats membres de prévenir et de réparer les violations de la Convention commises par des personnes ou des entités privées en vertu des conditions précitées.

3.4. Les Etats membres n'encouragent pas les intermédiaires internet, indépendamment ou collectivement, à surveiller et censurer les contenus qui ne sont considérés comme illicites ni par le droit international ni par le droit national.

4. Encourager des pratiques commerciales respectueuses des droits de l'homme chez les intermédiaires internet

4.1. Sachant que la relation entre les intermédiaires et les usagers relève pour l'essentiel du droit privé, les Etats membres incitent les intermédiaires internet à mettre en œuvre des pratiques commerciales respectueuses des droits de l'homme, en particulier de la liberté d'expression et de la protection des données.

4.2. Les Etats membres s'efforcent d'assurer que les contrats conclus entre les usagers et les intermédiaires soient conformes aux principes sous-jacents à la Convention (Khurshid Mustafa et Tarzibachi 2008, paragraphe 33, 16 ; Pla et Puncernau (2004), paragraphe 59).

4.3. Les Etats membres veillent à ce que les intermédiaires internet respectent la législation en matière de protection des données et de protection des consommateurs et, à cette fin, envisagent d'encourager le réexamen régulier des conditions de service, de la politique de monétisation des intermédiaires, de l'utilisation des données à caractère personnel, du champ des décisions par algorithmes (notamment les algorithmes d'actualités et de recherche), des procédures de signalement de contenus (qui doivent être claires et transparentes) et des critères décisionnels concernant les contenus signalés.

4.4. Les Etats encouragent la transparence et la responsabilité des intermédiaires internet et ne leur adressent des demandes de retrait de contenu ou d'autres demandes concernant les données de clients que si la loi le prévoit et si cette mesure est nécessaire dans une société démocratique.

4.5. Les Etats encouragent les intermédiaires à offrir aux usagers des moyens rapides et effectifs d'obtenir réparation en cas de réclamation ou de violation des conditions de service, et mettent en place des voies de recours effectives dans le cadre de leur système judiciaire national pour les cas où les mécanismes internes et les mécanismes alternatifs de règlement des litiges s'avèrent insuffisants.

4.6. Tout en respectant les droits des intermédiaires internet, les Etats membres œuvrent en faveur de l'évolution de la sphère publique en ligne. En particulier, lorsque les décisions des intermédiaires internet empêchent l'exercice effectif de la liberté d'expression, les Etats membres peuvent être amenés à protéger la jouissance des droits énoncés par la Convention en réglementant les droits de propriété de façon à préserver l'espace de communication offert par internet.

5. Questions de compétence soulevées par les activités des intermédiaires internet

5.1. La nature d'internet implique que les intermédiaires seront soumis à différents systèmes juridiques, ce qui peut avoir des effets dissuasifs en termes de contenus mis à disposition via les intermédiaires.

5.2. Les Etats membres veillent à ce que leur obligation de respecter, de protéger et de réaliser tous les droits et libertés consacrés par la Convention ne soit pas exercée d'une manière assimilable à un abus de procédure.

5.3. Reconnaissant l'égalité souveraine de tous les Etats membres et la marge d'appréciation dont ils disposent dans l'élaboration de leur cadre normatif, aucun Etat membre n'adopte de lois qui produisent des effets extraterritoriaux importants et injustifiés.

5.4. Les Etats membres n'introduisent aucune condition de localisation des données ni n'exigent de la part des intermédiaires internet qu'ils soient physiquement présents sur leur territoire.

5.5. Les Etats membres veillent à ce que les juridictions nationales se déclarent compétentes à l'égard des intermédiaires qui opèrent à l'étranger uniquement lorsque l'opération a une incidence suffisamment sérieuse sur un éventuel réclamant. Les parties privées ne devraient porter une affaire devant une juridiction que si elles peuvent établir qu'elles ont un lien réel et substantiel avec cette juridiction et qu'elles ont subi un préjudice grave dans son ressort.

5.6. Les Etats encouragent l'établissement d'un dialogue, dans les enceintes appropriées, pour résoudre les conflits de lois et de compétence.

ANNEXE 4[3]

Projet de rapport sur les dimensions des droits de l'homme dans le domaine des algorithmes

Draft report on the human rights dimensions of algorithms

RAPPORTEUR: BEN WAGNER
Director of the Centre for Internet & Human Rights
European University Viadrina, Frankfurt / Oder
Germany

Table of Contents

[3] Rapport tel que reproduit sous le document MSI-NET(2016)06 du 12 septembre 2016 – non disponible en Français

SUMMARY AND MAIN CONCLUSIONS

[Summary will be inserted here once a final version of the study has been completed]

1. INTRODUCTION

What information can you see on your Facebook feed? Who is a criminal or a terrorist? Will you get health insurance? Are we going to give you a job? Many of these questions used to be answered by human beings and are currently increasingly being answered by automated decision-making systems. These automated decision-making systems raise considerable challenges not only in each policy area they are used but also for societies as a whole on how to safeguard fundamental rights and human dignity in the face of rapidly changing technology. The right to free elections, workers' rights, the right to life, freedom of expression, privacy and even the rule of law itself are all impacted as will be shown in the following study. As such it is perhaps unsurprising that how to respond to challenges associated with 'algorithms' and Internet intermediaries is currently one of the most hotly debated public policy questions.

As "software is eating the world" (Andreessen 2011) human beings are increasingly surrounded by technical systems which make decisions that "they do not understand and have no control over" (Article 29 Data Protection Working Party 2013). While this can be disconcerting it is not necessarily a negative development but rather a product of this particular phase of modernity in which globalized economic and technological development produce large numbers of software-driven technical artefacts. These "coded objects" (Kitchin and Dodge 2011) embed all manner of decision making capacities that are relevant for public policy decision makers: Which split-second choices should a software-driven vehicle

make if it knows it is going to crash? Do the algorithms of quasi-monopolistic Internet companies have the power to tip elections? What rights do workers have whose entire relationship with their employer is automated? Is racial, ethnic or gender bias more likely in an automated system and how much bias should be considered acceptable?

None of these questions provide for easy public policy answers and yet decision makers can and should spend time trying to grapple with these challenges. Historically many of the decisions on how to develop these kinds of software have been made by private companies, following whichever economic, legal and ethical frameworks those companies saw fit. There is undoubtedly a deficit in well-founded public policy that provides a framework for the regulation of algorithmic decision making (systems and processes), but it is unclear whether effective regulation is possible while many technologies based on algorithms are still in their infancy. The issues arising from the use of algorithms in decision-making are manifold and complex and include concerns about data quality, privacy and unfair discrimination, but the debate is still at such an early stage that understanding what algorithms actually do and which consequences for society flow from them may be difficult to discern at this stage. This should not however prevent more fundamental deliberations on how human rights should be secured in a world governed by algorithmic decision-making at a more principle based level. Concerns need to be identified and thought should be given to how these concerns could potentially be addressed by the normative framework.

This is particularly the case as many public policy initiatives in this area are quickly copied by other states around the world, leading to relatively swift cascades of good or bad policy. Moreover, many of the debates about algorithms focus less on algorithms themselves and more broadly on the role of technology in society (Bucher 2016). While many of the elements of debates on technology and society are important in understanding algorithms (Bijker et al. 2012), there are also novel policy challenges that arise in debates about algorithms which are related to automated (or semi-automated) decision-making. These challenges will form the core of this study which we hope will be able to shed some light on the human rights dimensions of algorithms.

2. DEFINING ALGORITHMS AND AUTOMATED DATA PROCESSING TECHNIQUES

When looking at algorithms and the automated data processing techniques they engage in, it is important to be absolutely clear what types of algorithms are being discussed here. Rather than reinventing the wheel, this study will build on existing well-established definitions used by other authors, in particular the work of Tarleton Gillespie (2014), Nicholas Diakopoulos (2015) and Frank Pasquale (2015).

This definition used here starts from Tarleton Gillespie's assumption that "algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations. The procedures name both a problem and the steps by which it should be solved." (Gillespie 2014:167) Thus it can be suggested that algorithms are "a series of steps undertaken in order to solve a particular problem or accomplish a defined outcome." (Diakopoulos 2015:400).

However saying what algorithms *are* is not the same as defining which algorithms matter. For the purpose of this report it seems reasonable to limit the scope of the algorithms being discussed to those which are digital (Diakopoulos 2015) and are of "public relevance" (Gillespie 2014:168). Moreover in order to separate out the specific human rights dimensions of algorithms, this report will focus on algorithmic decision-making, i.e. when algorithms make decisions in an automated or semi-automated fashion

[1] This type of decision-making is often subjective in that there is no obvious right or wrong answer but rather the judgement of a human being was previously used to make a subjective determination that is now being made by an automated system (Pasquale 2015:8).

Finally it should be noted that algorithms as discussed here do not exist meaningfully without interaction with human beings. They are deeply entangled with practice (Gillespie 2014:168) and the "promise of algorithmic objectivity" (Gillespie 2014:168), both of which serve to create the social and institutional conditions in which algorithms have effects on real life human beings. It is heavily misleading to claim the computing systems are or even can be neutral, rather technologies are deeply social constructs (Winner 1980, 1986) with considerable political implications (Denardis 2012). Thus when the 'computer says no'[2] the decision-making software in the computer is "biased but ambivalent" (McCarthy 2011:90), it has no meaning without a social system around it that gives this 'no' meaning. It is thus too simple to simply blame the algorithm and simply suggesting to stop using computers or computing is rarely a helpful alternative. Rather specific norms and values are embedded in and enmeshed with algorithms that need to be questioned, critiqued and challenged.

Thus is should be evident that many of the decision making processes around algorithms are relevant for scrutiny by policy makers. However for the purposes of this study this ascertain is not sufficient, it is also important to ask to whether algorithms have an impact on human rights?

The French Parliament certainly seems to think so. "On 26 January 2016, the French National Assembly voted for a new Bill on digital rights. The Bill includes provisions relating to algorithmic transparency and the duty of 'loyalty', or fairness, of online platforms and algorithmic decision-making" (Rosnay 2016). Beyond France there are numerous indications that algorithms do indeed have an impact on human rights. The longest and most sustained human rights debate on algorithms and automated data processing relates to the Right to Privacy (Tene and Polonetsky 2013). It is possible to find articles from more than 45 years ago which discuss infringements of the right to privacy (Sills 1970) associated with automated data processing. Moreover data protection regulation such as the EU's General Data Protection Regulation has also produced some of the key regulatory instruments for algorithms such as the "right to explanation" (Goodman and Flaxman 2016) or the right of access to "knowledge of the logic involved in any automatic processing of data concerning him" (EU Directive 95/46/EC). However one of the main challenges faced in this area is that data protection is often understood in an individual rather than a collective sense (Mantelero 2016), which suggests a false sense of agency for individuals. It can also be seen in this context that the European Data Protection Supervisor (EDPS) appointed an Ethics Advisory Group to go beyond the boundaries of existing Data Protection law to search for a new Digital Ethics.[3]

Another human right that is evidently affected by the usage of algorithms is Freedom of Expression. The report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the Thirty-second session of the Human Rights Council (A/HRC/32/ 38) suggests that "search engine algorithms dictate what users see and in what priority, and they may be manipulated to restrict or prioritize content"

---

[1] The distinction between 'semi-automated' and 'solely automated' is important and exists in various EU Directors on data protection such as the GDPR. For the purposes of this study we will – following similar work on this topic by the Council of Europe - not differentiate but consider both semi-automated and solely automated decision-making as relevant automated decision-making processes.

[2] See https://www.youtube.com/watch?v=AJQ3TM-p2QI for a full explanation of this phrase.

[3] See https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Ethics for further details.

(Kaye 2016:7) and that "platforms deploy algorithmic predictions of user preferences and consequently guide the advertisements individuals might see, how their social media feeds are arranged and the order in which search results appear" (Kaye 2016:16).

Another key fundamental freedom that is frequently cited in relation to human rights is the right to Protection against Discrimination. Various discriminatory patterns arise around the usage of algorithms that are frequently suggested to violate this right (Caliskan-Islam, Bryson, and Narayanan 2016; Tufekci et al. 2015). There are also suggestions that certain forms of algorithmic decision-making lead to "social sorting" (Lyon 2003).

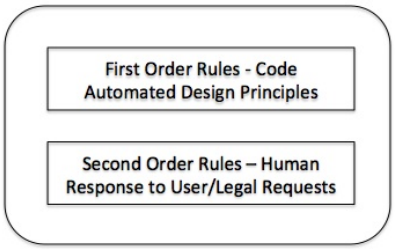
Beyond these three fundamental rights discussed above, there are numerous other areas in which human rights may be affected by algorithms. These include ensuring the rule of law (Pasquale 2015; Joerden 2015), the right to free elections (Bond et al. 2012), workers' rights (Irani 2015) and even the Right to Life (Asaro 2013). A similar elaboration could be made for almost any other human right, but suffice to say at this point that there are evidently human rights aspects to the usage of algorithms and that they are thus worthy of further study by policy makers to understand these aspects.

3. CHARACTERISTICS AND LIMITATIONS OF ALGORITHMS

There are many different aspects that can be considered as key characteristics of algorithms that engage in automated data processing and (semi-)automated decision making. As a result this list cannot be exhaustive or predict all possible potential iterations of algorithms and their decision-making. Rather it attempts to provide an overview of the current characteristics and limitations traits of algorithms in 2016.

Automation is one of the core challenges associated with algorithmic decision-making. The ability of automated computing systems to make decisions about a growing number of situations previously decided by human-beings is a key characteristic of the practical implementation of algorithms. It is important to note in this context that human decision-making and algorithmic decision-making is fundamentally different (Spiekermann 2015). While algorithmic decision-making is increasingly adept at mimicking the decision making of human beings, important elements (such as discretion) of decision-making processes cannot be automated and often get 'lost on the way' when human decision-making processes are automated (Spiekermann 2015). This is not to say that decision-making by humans or algorithms is necessarily better or worse, but rather that the two are fundamentally and categorically different, have different kinds of consequences and make different kinds of mistakes. While societies and governments around the world have considerable experience understanding human decision-making and its failures, we are only beginning to understand algorithmic decision-making and its flaws.

Another important aspect of algorithmic decision making is their perceived inflexibility in some areas and their incredible flexibility in others. Broadly speaking, algorithms are typically highly adaptive within the scope of their programming and are typically able to integrate considerable amounts of additional data without great difficulty. In order to simplify this statement the graph on the left may help to explain the adaptive nature of algorithms. Without any changes to the actual code the data processing (first order rules) of algorithms is typically more difficult to influence than the outputs of algorithms (second order rules) (Wagner 2016a). This distinction is important, as the first order elements of automated decision-making processes are often adaptive, and can adjust to second order rules very rapidly (Wagner 2016b).



One area where algorithms are typically very inflexible (where the computer says 'no') is in the area of procedural and deeper structural changes to their decision making, or first order rules as they are termed here. This characteristic can often be observed with organisations which implement algorithmic systems without an in-house capacity to change the software code themselves. Even if the outputs of the system are perceived as 'mistakes' it will often be easier and/or cheaper for such organisations to 'fix' the problem with second order rules rather than to change the algorithm itself. Problems about algorithmic flexibility or inflexibility have little to do with the actual algorithms themselves but instead are a product of how human beings implement and regulate algorithms.

In relation to flexibility another aspect of some algorithms design also needs to be considered, namely self-learning or adaptive algorithms. There algorithms have the ability to learn based on data they receive through machine learning techniques (Williamson 2016). This ability to learn new 'tricks' from the data they receive certainly makes algorithms more flexible in some regard, but also makes their output harder to predict (Gillespie 2016). This also has led some authors to suggest that many forms of algorithmic transparency, accountability and regulation are impossible because the programmers themselves are unable to predict or fully understand how the algorithm makes the decisions that it makes (Kroll 2016).

Finally many technologies based on algorithms use data mining and pattern recognition without "understanding" causal relationships (correlation instead of causation), which may lead to errors and raise concerns about data quality. Related to this, one key challenge linked to the implementation of algorithms is the frequent perception that they are able to create neutral and independent predictions about future events. The hype around Google Flu trends in 2011 which later turned out to be completely unjustified as their prediction ability was far lower than claimed is just one example of the ongoing struggle with claims around predictive algorithms (Lazer et al. 2014; Lazer and Kennedy 2015). The challenge however is less to do with algorithms themselves and far more about how human beings perceive and interpret their results. The belief that computer algorithms produce neutral unbiased results (Chun 2006) without any form of politics (Denardis 2008) is at the heart of this problem. Rather than changing the algorithms in any way, it would be far more helpful to ensure more critical engagement in public debates about them.

4. EMPIRICAL DIMENSIONS: CURRENT AND FUTURE USES OF ALGORITHMS

The following set of cases provides a broad overview of the areas in which automated decision-making is currently employed in a way which raises relevant public policy questions. However this list is not exhaustive and is based primarily on those areas in which considerable public, academic or expert debate already exists and thus some preliminary comparisons and conclusions are possible. Areas that could have also been covered in this context include healthcare, mobility and many other areas that are not even being debated yet but may be in future.

A. CONTENT FILTERING AND WEBSITE BLOCKING

One of the key public policy debates about online content filtering is the extent to which content removal by social media platforms takes places manually, semi-automatically or automatically. While large social media platforms like Google or Facebook love to claim that all content taken down is previously reviewed by a human being (Buni and Chemaly 2016), there are evidently large parts of the process which are automated (Wagner 2016b). Given

the importance of platforms like Google or Facebook, their centrality for many users experience of the Internet as a quasi-public sphere (York 2010) and their ability to massively amplify certain voices (Bucher 2012) this is by no means a trivial matter.

Automation of the content removal process by social media platforms is particularly evident in the response times that different types of content receive and how content is prioritized, a process that is evidently automated. The same goes for the threshold of user complaints that are required before a piece of content is reviewed. While this varies for different kinds of content it is not 0 and there are strong suggestions that the complete responses of Facebook to user queries is automated for many types of content (Wagner 2016b; Zhang, Stalla-Bourdillon, and Gilbert 2016). Thus it is possible that many users complain about a specific type of content without an automated algorithm judging it relevant to ask a human operator to review the content. As a result, it is possible to claim that large parts of the content takedown process are automated and the even human content takedowns are at minimum semi-automated. Another example are 'upload filters,' which are used to scan for and automatically remove content considered copyright infringement or child sexual abuse images (McIntyre 2012). It has been suggested that similar algorithms could be used for extremist content (Toor 2016).

As noted by Tufekci et al. (2015) "The scale of the content on user-generated platforms and costs associated with human moderation are the reasons algorithmic processes appeal to platforms. Yet, given the crucial gate-keeping function played by these platforms, algorithms also introduce new complications rather than creating a simple solution." Thus many of the practices discussed above involved algorithmic decision-making and thus pose considerable challenges for the rights to Freedom of Expression and Privacy.

B. TERRORISM AND CRIME PREVENTION

There has been a considerable push for the usage of automated decision-making in the areas of national security and crime prevention. Following a string of violent attacks in the US and Europe in recent years, many European and US politicians have begun calling for online social media platforms to use their algorithms to identify terrorists (Rifkind 2014; Toor 2016). Many social media platforms are seemingly already using algorithms to identify extremist content and are being asked by governments to pass on the results generated by these algorithms to governments. One important example of this practice relates to British parliamentary investigation into the murder of the British soldier Lee Rigby in London 2013.

According to a report from the British Intelligence and Security Committee of Parliament the killers had, apparently, posted extremist content in an online social network that was flagged and removed, reportedly algorithmically. The Parliamentary report states that: "The Committee asked GCHQ about the processes by which companies hosting such platforms might close accounts. GCHQ explained that different Communications Service Providers (CSPs) use different systems. However, it appears that there are: various automated techniques for identifying accounts which they believe break their terms of service. They use these techniques to identify and disable accounts which they believe may be linked to child exploitation and to illegal acts such as inciting violence […] Such accounts are then automatically suspended." (Rifkind 2014)

In the US, the Obama administration has advocated for the use of 'hashes'[4] for the detection and automatic removal of extremist videos and images. Additionally, there have been proposals to modify search algorithms in order to "hide" websites that would incite and support extremism. The hash mechanism has been adopted by Facebook and YouTube for video content, however no information has been released over the presence of human input nor on the criteria adopted to establish which videos are "extremist". In Europe, while similar projects are under scrutiny, the Interpol has created a regional organization monitoring online extremist content called the "Internet Referral Unit". The system will be automated in the next few months with the introduction of the "Joint Referral Platform."[5] Notably the data on extremist online content that Europol is processing refers not just to Internet content which is illegal in Europe or one of its member states but also to material which violates the Terms of Service of an Internet intermediary. By contrast the Internet Referral Unit of the Netherlands have publicly stated that they have no interest in policing the Terms of Service of Internet Intermediaries and "don't do anything automated" (Lestrade 2016).

In a different vein, it should also be noted that automated recommender systems can also have problematic effects in regards to ideological or political content. Specifically, the programming of many online recommendation systems can create 'filter bubbles' - fully-automated echo chambers in which individuals only see pieces or information which confirm their own existing opinions - of extremist content (Bozdag 2013; Pariser 2011; Zuckerman 2013) which according to the results of recent research are relatively easy to stumble into and relatively hard to get out of (Salamatian 2014). These fully-automated echo chambers pose the danger of creating "ideological bubbles" (O'Callaghan et al. 2014) of online content. However other scholars like Borgesius et al. who argue that there is "there is little empirical evidence that warrants any worries about filter bubbles" (Zuiderveen Borgesius et al. 2016).

Moving from terrorism to crime prevention, the main policy debates around the usage of algorithms seem to be related to the concept of predictive policing. This approach - broadly framed – bases its analysis on historical patterns of crime to predict future patterns of crime beyond the ability of human beings. This has included developed automated systems which predict which individuals are likely to become involved in a crime (Perry 2013). Similarly, to the online content algorithms discussed above, there is considerable concern that these recommender systems for crime are likely to create echo chambers within which existing biases and prejudices are sedimented. Existing biases and prejudices related to for example racial or ethics groups are then not recognized by the police as their own biases, as they have become integrated into an automated computer program. As the computer program is perceived to be independent and neutral, these biases become 'normal' and part of everyday usage of a computer, rather than specific decisions of an individual which can be more readily questioned.

C. SEARCH ALGORITHMS AND SEARCH FUNCTIONALITY MORE GENERALLY

Search algorithms and search functionality more generally form a key aspect of the Internet. The ability to search the Internet would however be impossible without search algorithms that provide responses to user queries. Search algorithms can be horizontal or vertical in nature. Horizontal search algorithms are used for general search. For instance, the search engine providers Google and Bing employ horizontal search algorithms for general search; to

[4] Hashes are unique identifiers for pieces of internet content that are typically generated by an algorithm and simplify the identification process. For a further explanation of what hashes are and how they are used to regulate internet content see (McIntyre 2012).
[5] Submission from Article 19.

help web users locate particular information from millions of web pages.[6] Vertical search algorithms (otherwise known as specialised search algorithms) are used to search *"a specific segment of online content"* (Verhaert, 2014, p. 266). Moreover most modern search tend to provide personalized results which adapt the search results to the algorithmically predicted preferences of their users (and this creates the potential filter bubble).

Search algorithms and search engines are likely to have a positive impact on the fundamental right to freedom of expression. As observed by the Committee of Ministers of the Council of Europe: "*Search engines enable a worldwide public to seek, receive and impart information and ideas and other content in particular to acquire knowledge, engage in debate and participate in democratic processes.*"[7]

However search algorithms and search engines may also have a negative impact on freedom of expression. Content which is not indexed or not ranked highly by one of the few popular internet search engines may be less likely to reach a large audience. A search algorithm might also be biased towards certain types of content or content providers, thereby risking to affect related values such as media pluralism and diversity.[8] This can lead to considerable discrimination issues, both in regards to end-users, customers and societies as a whole.[9] A biased algorithm within a large quasi-monopolistic search engine that systematically discriminates one group in society based on their age, sexuality, race or gender would cause considerable problems not just for the individuals affected by these decisions, but for societies as a whole.

There are also concerns with search engines impact on the right to privacy and data protection. The specific dimensions of this impact relate to facilitating aggregation through gathering information about a specific individual, reducing practical obscurity by making it easier to find information about an individual, violating contextual integrity by violating norms about the distribution of information and reducing individual control over information disclosure as a whole.[10]

D. SURVEILLANCE, ONLINE TRACKING, PROFILING AND "SOCIAL SORTING"

Algorithms play a role in online tracking and profiling of individuals whose browsing patterns are recorded on the basis of cookies and similar technologies such as digital fingerprinting and aggregated with search queries (search engines) and other data (eg social media tracking and data collection through apps on mobile devices) (Tene and Polonetsky 2012). One of the main applications of online tracking and profiling is targeted advertising based on the profile of presumed interests of the person tracked. However these profiles can also be used in the context of assessing a person's risk profile for the purpose of insurance or credit scoring (discussed further below) or more generally for differential pricing (offering different prices for the same goods or services to different consumers, based on their profile). Particular concerns arise from the use of data brokers who aggregate the information contained in personal profiles and this information may then be mined through the use of algorithms, which creates a risk of large-scale surveillance (dataveillance) by private entities and governments alike (Rubinstein, Lee, and Schwartz 2008). The major problem of using data from profiles for different purposes through algorithms is that the data loses its original

[6] Submission from Sophie Stalla-Bourdillon, Steffen Staab and Laura Carmichael.
[7] Council of Europe, Recommendation of the Committee of Ministers to member States on the protection of human rights with regard to search engines, CM/Rec(2012)3, Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies, paragraph 1, available at https://wcd.coe.int/ViewDoc.jsp?id=1929429.
[8] Submission from Aleksandra Kuczerawy, Brendan van Alsenoy and Jef Ausloos.
[9] Submission from Sophie Stalla-Bourdillon, Steffen Staab and Laura Carmichael.
[10] Submission from Aleksandra Kuczerawy, Brendan van Alsenoy and Jef Ausloos.

context and this use is therefore likely to affect a person's informational self-determination and is likely to be prejudicial and/or discriminatory, as the data loses its contextual integrity (Nissenbaum 2004; Tene and Polonetsky 2012). Furthermore the use of algorithms on aggregated profile data may also increase undesirable social inequalities (for example power, status, wealth) (Tene and Polonetsky 2012). This has already been described as 'social sorting' (Lyon 2003).[11]

a. From a human rights point of view some of these concerns can be addressed through developing the right to privacy, but other concerns are not sufficiently captured by the right to privacy. Thus, some scholars have argued that from a normative point of view more conceptualisation of these concerns is required to develop the framework of normative principles further, for example as part of a fundamental right not to be unfairly discriminated against. Others have suggested that this right is already sufficiently covered by Article 14 of the European Convention on Human Rights on anti-discrimination which just needs to be applied more broadly.

E. INSURANCE AND CREDIT SCORING

The objective of insurance is to provide a degree of "financial protection" (David, 2015, p. 147) to the applicant(s). Insurance risk assessment is a formal statistical method utilised to assign applicants to appropriate insurance tariffs by considering the likelihood, frequency and cost of a potential claim (David, 2015, p. 148). Prior to the use of formal statistical methods, "subjective human assessment" was used for creditworthiness assessment (Hand & Henley, 1997, p. 530) and insurance; i.e. the examination of an individual's application on a case-by-case basis. However, the current credit scoring model faces a number of criticisms – principally they lack transparency and assess a limited range of variables.[12]

In some instances, algorithmic credit scoring aims to focus beyond traditional variables and take advantage of additional types and amounts of data, such as social media data (Williams 2016) and browsing history to further enrich creditworthiness assessment (Holloman, 2014), (Shipley & Zhuo, 2016), (Clements, 2015). Credit scoring has a potentially broader remit than was initially intended; e.g. it is not only used by lenders but employers (The Editorial Board, 2013).[13] Many businesses traditionally working in the field of credit scoring have expanded their reach to become data brokers and identity management companies (for example providing age-verification information).

F. AUTOMATING THE WORKPLACE AND WORKERS RIGHTS

The workplace is another key area whether automated decision making has become increasingly common in recent hears. Algorithms are increasingly involved in decisions on both hiring and firing staff, staff organization and management as well as evaluating the professional contribution of individual staff members (Tufekci et al. 2015). These decision-making processes are by no means perfect when they are conducted by humans and there are numerous biases in hiring related to race (Bertrand and Mullainathan 2004) class and gender (Altonji and Blank 1999; Goldin and Rouse 1997) that have been demonstrated. With more and more companies moving towards algorithmic hiring (Rosenblat, Kneese, and others 2014) it is however highly problematic that the systems employed typically lack any transparency in the decisions they make, both in the hiring process and beyond. Moreover

[11] Submission from Julia Hornle.
[12] Submission from Sophie Stalla-Bourdillon, Steffen Staab and Laura Carmichael.
[13] Submission from Sophie Stalla-Bourdillon, Steffen Staab and Laura Carmichael.

many of these automated decision-making processes are based on data from Internet intermediaries.

Another challenge is related to automated feedback loops which decide how employees should be managed and are typically linked to customer input (Kocher and Hensel 2016). By allowing the 'wisdom of the crowd' to make decisions about individuals employment is not only highly ethically questionable, it also limits the ability of workers to contest such decisions as they seem to be 'objective' measures of their performance. As individual employment platforms are "Transforming People into Human Computation" there are obvious questions to be asked about workers' rights, employee self-determination and how societies as a whole believe that human beings should be treated at the workplace.

G. CLOUD PROVIDERS AND DATA STORAGE

Another key aspect related to the usage of algorithms for automated data processing focusses on 'cloud' data storage. This refers to solutions whereby files and other data are no longer stored on local storage but are stored remotely on servers accessible via the Internet. However by virtue of engaging in non-local storage practices, the data of users is also subject to being processed by algorithms while stored remotely in ways that would not be the case if the information is stored remotely. There are two places where such automated data processing can take place: (1) in transit to the remote network storage location and (2) on the remote servers where the data is stored. Importantly as modern operating systems are increasingly deeply enmeshes with 'cloud' i.e. remote services, it is increasingly difficult for users to ascertain to what extent they are using local or remote services. For example, the Siri service for voice interaction with users phones regularly interacts with and stores data on remote servers (Yamamoto et al. 2014) without this being evident let alone transparent to users (Article 29 Data Protection Working Party 2013).

The key question in regards to data in transit is whether it is sufficiently protected or not through technologies such as strong end-to-end encryption [Schulz and Hoboken forthcoming]. If data is encrypted automated data processing becomes a lot more difficult and in some cases completely impossible. If the data which is transferred to the cloud is not encrypted - as is surprisingly common even though this should not be the case – then whichever networks the data passes can analyze and even modify the data. Actors doing so range from intelligence services such as the U.S. NSA or the British GCHQ to more mundane peddlers of advertising such as Phorm and NebuAd (Ermert 2013; Greenwald and MacAskill 2013; Metz 2008; Williams 2008).

However this does not mean that cloud data is safe simply because it is encrypted in transit. It is also possible for data to be manipulated and analyzed on the servers where it is being stored. For example, Microsoft's cloud service 'SkyDrive' operates an "automated process designed to pull the trigger when it 'sees' certain content (such as nudity)," leading to a users account being terminated when such content is found (Clay 2012). This is particularly problematic for many users who "believe their images to be private" (Heckert 2011) are now confronted with an unwanted automated decisions being made based on their personal data.

H. ELECTIONS & IMPLICATIONS FOR DEMOCRACY

[Include cross-link and reference to CoE MSI-MED Report by Damian Tambini].

One important area that is often ignored when looking at the effects of automated data processing and algorithms relates to elections. Since the advent of the Internet it has been

argued that online campaigning and social media were likely to change the way in which politics and elections work but it is only more recently that academic research has revealed the extent to which changes to online content platforms can 'tip' elections. More specifically researchers manipulated the Facebook platform without users knowledge during U.S. elections and were thus able to convince a statistically significant segment of the population to vote (Bond et al. 2012). There are strong indications that since then Facebook has been selling similar services to political parties around the world, with similar behaviour observed during the UK local elections in 2016 (Griffin 2016). Whether Facebook and similar quasi-monopolistic online platforms are using their power to influence human voting benevolently or not is less the point than the fact that they – in principle – have the ability to massively influence elections.

At the same time Facebook is increasingly considered by scholars such as Helberger et al. to be acting as a "news editor [that] has editorial responsibility for its trending topics" (Helberger and Trilling 2016). This in turn begs the question of whether social media platforms should be considered Internet intermediaries or rather the editors of news websites.

I. INTERNET OF THINGS AND SMART CITIES

As discussed in the introduction the spread of programmed objects into all areas of society and human life is being increasingly common. This shift which is sometimes referred to as the 'Internet of Things' or discussed in the context of 'smart cities.' With increasing amount of automation and larger amounts of data that is typically stored by Internet intermediaries it is in theory possible to better tailor automated systems surrounding human beings to their needs. However it is an open question whether such automated systems are used in the interests of users or citizens, particularly when they are implemented in highly sensitive areas such as the medical sector (Bates et al. 2014).

As noted by Natali Helberger "there are possible challenges from the Internet of Things for the 'profiled consumer.' These challenges go beyond issues of privacy and data protection – which will continue to play a prominent role. In addition, the protection of contractual fairness, adequate information and autonomous and free choices comes to the fore" (Helberger 2016:22) Finally it is very common for the data collected by such services to be shared between different data brokers (Hoofnagle 2003), ensuring that the 'profiled consumer' becomes a 'profiled citizen.'

J. DIGITISATION OF PUBLIC SECTOR & GOVERNMENT SERVICES

Numerous government agencies and services are increasingly automating their decision-making with the use of algorithms. While it is heavily debated whether such systems can increase efficiency or not what is evident is that many of the systems pose considerable questions for transparency and accountability of public decision-making. This is particularly the case as these are government authorities which are typically held to a higher standard in their decision making than private sector or other non-governmental organisations.

Despite these standards there are strong suggestions that the public sector is employing automated-decision making in areas as diverse as social security, taxation, health care and the justice system. For example many courts in the United States use a computer program to assess the risk of repeat offending, which has been shown to be "biased against blacks" (Kirchner 2016). Another example relates to the practice of *Profiling the Unemployed in Poland* (Jędrzej Niklas, Karolina Sztandar-Sztanderska, and Katarzyna Szymielewicz 2015).

During their analysis they identified several challenges which are broadly also true for the usage of algorithms in other areas of the public sector service delivery as well:

> *"1.Non-transparent rules of distributing public services […]*
>
> *2. Shortcomings of computer systems as a trigger for arbitrary decisions …]*
>
> *3. Gap between declared goals and practice […]*
>
> *4. System based on the 'presumption of guilt' […]*
>
> *5. Categorization as a source of social stigma […]*
>
> *6. Risk of discrimination" (Jędrzej Niklas et al. 2015:33–37)*

Finally there are risked associated with outsourcing key government functions such as the provision of government benefits to the private sector. It has been argued in South Africa that operating such privatized government services while simultaneously engaging in competitive banking and insurance markets provides an inappropriate competitive advantage to companies who operate privatized government services (Elza Van Lingen 2016). Aside from the competition concerns there are evident concerns related to privacy and data protection that also arise from such arrangements, particularly as many of the organisations providing these kinds of services are Internet intermediaries.

5. ETHICAL & LEGAL & HUMAN RIGHTS DIMENSIONS

Many of the challenges discussed above touch upon, ethical, legal and human rights challenges. None of these challenges are easily or readily resolved, not should regulatory responses to algorithms and automation be taken lightly. Importantly many of the challenges related to automated data processing have historically been resolved by data protection legislation. Thus relevant innovative governance mechanisms such as the "right to explanation" (Goodman and Flaxman 2016) are also typically the product of data protection legislation. However it should be noted that there is a significant difference between the right to privacy and the data protection regulation, which is at the end still a governance mechanism to safeguard privacy and other rights. Moreover it should be evident from the previous analysis that the "challenges go beyond issues of privacy and data protection" (Helberger 2016:22) and thus cannot be resolved by recourse to data protection regulation alone.

Challenges around discrimination of content raises questions of competition law and discrimination of minorities, while the ability of algorithms to manipulate elections is a matter for electoral commissions and parliaments. There are also issues related to "protection of contractual fairness, adequate information and autonomous and free choices" (Helberger 2016:22). While the issues touched upon above are too broad to be covered by data protection regulation alone, nor should these regulatory mechanisms or the expertise of the data protection community be forgotten in the process of finding regulatory responses to algorithmic governance.

Importantly there is a danger that if misconstrued some of the statements or recommendations in this report could be used to regulate the development of algorithms or other software code. So to be absolutely clear it should be stated here that this should is not a reasonable outcome of this report and any such interpretation would be false. This is because interference with the right of individuals to research, develop and test would itself

be a grave infringement of human rights and in particular freedom of opinion, expression, thought and research. Aside from significant human rights impacts of doing so, limiting research and development of algorithms actually limits a better understanding of how algorithms operate and what effects they have. Importantly many of the public policy solutions can only that will be discussed below are only relevant for very large actors with a considerable quasi-monopolistic market share (Naughton 2016) and could well be harmful if implemented on implementers of algorithms of all shapes and sizes.

Finally, there are very fundamental legal and ethical surrounding the legal personhood of automated systems such as algorithms that cannot easily be resolved in this report. Particularly around questions such as liability and accountability these questions are important, not in a manner to exculpate those involved in developed and implementing such systems from responsibility but rather to acknowledge that accountability and liability is becoming increasingly complex with autonomous systems.

6. MECHANISMS OF GOVERNANCE, ACCOUNTABILITY & TRANSPARENCY

There is a frequently stated perception that the regulation of algorithms in automated systems is either impossible or extremely difficult. Such statements tend to ignore the numerous cases in which algorithms are already regulated before their implementation by government regulators or independent auditors. To provide just one example, the software and algorithms used in 'slot machines' in Australia and New Zealand are required by government regulation to be "fair, secure and auditable" (Woolley et al. 2013). As part of this process the developers of such machines are required to submit their algorithms to regulators before they can be presented to consumers. The same applies to the regulation of online gambling in the United Kingdom, where gambling equipment is controlled by a specific licensing regime.

The Australian/New Zealand Gaming Machine National Standard in its most recent revision 10.3 defines in extraordinary detail the technical specifications by which such machines can operate. For example the "Nominal Standard Deviation (NSD) of a game must be no greater than 15" and "the hashing algorithm for the verification of gaming equipment software, firmware and PSDs is the HMAC-SHA1 algorithm".[14] This is not to say that such mechanisms would definitely be appropriate for regulating Internet intermediaries, but rather that the claim that the regulation of algorithms is impossible is evidently false and that regulators should look to existing mechanisms already implemented.

A. TRANSPARENCY

One of the main challenges frequently cited in regulating algorithms is that they seem like black boxes to both consumers and regulators (Pasquale 2015). As Tufekci et al note: "a common ethical concern about algorithmic decision-making is the opaque nature of many algorithms. When algorithms are employed to make straightforward decisions, such as in the case of medical diagnostics or aviation, a lack of transparency raises important question of accountability" (Tufekci et al. 2015:11). Thus there is a frequent and growing debate about algorithmic transparency in which algorithms could be provided to independent auditors, regulators or the general public (Diakopoulos 2015; Rosnay 2016).

As provision of entire algorithms to the public is typically considered unlikely, there is also a debate around the possibility of providing key subsets of information about the algorithms to

[14] The Australian/New Zealand Gaming Machine National Standard which is available here: https://publications.qld.gov.au/dataset/a-nz-gaming-machine-national-standards

the public, for example which variables are in use, the average values and standard deviations of the results produced or the amount and type of data being processed by the algorithm.

All of these measures aim to increase transparency of automated systems. This is obviously complicated by the frequent changes in the algorithms used, as Google for example changes its algorithm hundreds of times per year (Tufekci et al. 2015). There is also the frequently danger of manipulation and 'gaming' or algorithms if they were made public. At the same time the usage of machine learning complicates transparency to a point where provision of all of the source code of an algorithm may not even be sufficient, and instead there is a need for an actual explanation of how the results of an algorithm were produced. Initial steps to such a right can be drawn from the European General Data Protection Regulation (GDPR) including a right to explanation (Goodman and Flaxman 2016).

Private companies also regard their algorithm as their key trade secret and hence disclosure is unrealistic. Besides, in a decision of 28 January 2014, the German Federal Supreme Court (Bundesgerichtshof) rejected a claim for information concerning the credit agency's algorithm as it was a protected business secret but allowed a claim for information concerning the data used to calculate creditworthiness through the means of the algorithm. However where algorithms are used in decision-making which potentially prejudices the rights of individuals an oversight mechanism may ensure that the algorithm operates in a fair and sustainable manner. An example for this is section 28 b of the German Federal Law on Data Protection which provides that there has to be a scientifically proven mathematical-statistical process for the calculation of the probability of a specific behaviour of an individual before such an algorithm can be used for making a decision about a contract.

B. ACCOUNTABILITY

What accountability do individuals have for the algorithms they implement? This depends very much on the nature of the algorithms and their outputs. In many cases if the outputs are defamatory, infringe copyright or raise other legal concerns there are already governance mechanisms to ensure that these kinds of outputs are limited (Staab, Stalla-Bourdillon, and Carmichael 2016), with the case of Max Mosley taking action against Google just one of many examples (Stanley 2011). However such mechanisms typically only affect second order rules, i.e. changes to the outputs of algorithms. By contrasts there is a general lack of regulatory frameworks to influence first order rules and ensure that algorithms – in most cases – are actually producing results that uphold and protect fundamental values or basic ethical and societal principles.

However it has been suggested that "[t]echnologists think about trust and assurance for computer systems a bit different from policymakers, seeking strong formal guarantees or trustworthy digital evidence that a system works as it is intended to or complies with a rule or policy objective rather than simple assurances that a piece of software acts in a certain way." (Kroll et al. 2016)

This in turn feeds into the wider debate on auditing of algorithms by which 'zero knowledge proofs' could conceivably be generated by algorithms to demonstrate that they conform to certain properties without the individual engaging in the proof being able to see the actual algorithm (Kroll 2016).

7. REGULATING ALGORITHMS DIRECTLY

As was discussed above, gambling is one area where the code of algorithms is regulated directly and required to conform to certain standards, but it is not the only area where this kind of regulation is being discussed. In the financial sector there is an ongoing debate about the regulation of high-speed trading algorithms as these are seen to have a strong potential destabilizing effect on the overall financial system. One of the leading social democrat politicians suggested in 2012 that financial trading "algorithms will have to undergo a stress test to ascertain its stability" (Steinbrück 2012).

One associated area where similar regulation has been threatened is in the area of online content regulation and Internet hotlines. Here the British Police special unit CEOP demanded that their 'Facebook button' be provided by default to all Internet users (Wagner 2016b). While this attempt to pressure Facebook into changing its default code on the British Facebook website was unsuccessful, it suggests what kind of regulatory responses could be expected if states begin to define the content of algorithms on large online platforms.

Aside from direct regulatory mechanisms to influence the code of algorithms, indirect mechanisms to influence algorithms code could also be considered. These address the production process or the producers of algorithms and attempt to ensure they are aware of the legal challenges, ethical dilemmas and human rights concerns raised by automated decision-making. Another instrument to achieve such goals could be consist of standardized professional ethics or forms of licensing system for data engineers and algorithm designers similar to those that exist for professions like doctors, lawyers or architects.[15]

In conclusion it should be noted that the approach to direct regulation of algorithms or software code should be pursued with extreme care. It is the regulatory approach that provides the most pitfalls and is most likely to wider problems. Notably the direct regulatory approach raises considerable concerns about freedom of opinion and expression, the right to privacy as well as Freedom of Profession. Moreover given the fact that regulators currently do not know that much about algorithms, greater steps towards transparency and accountability of algorithms would seem far more appropriate.

8. CONCLUSIONS AND RECOMMENDATIONS

Understanding how automated decision-making systems operate is fraught with great difficulty and raises numerous public policy questions. None of these questions have easy answers, this should not however dissuade policy makers from looking more closely at them. Many of these challenges are so difficult to assess because the field is comparatively new and finding effective solutions remains difficult. As a first step it seems reasonable to suggest that policy-makers should seek to learn more about the implementation of automated decision-making systems in their respective countries. As a second step, they should try to ensure that existing law and legal frameworks remain implemented and effective in response to the challenges posed by automated decision-making in numerous different areas. As a final step, policy makers should be wary of limiting researchers or those trying to understand how algorithms operate, or focussing their regulatory efforts on organisations with low market share. This is because many of the policy challenges raised in areas such as free and fair elections or online content moderation only come into being by virtue of quasi-monopolistic markets.

[15] Submission from Markus Oermann, University of Hamburg.

Despite this MSI-NET have tried to develop some basic recommendations which we hope can help more the debate forward on effective public policy responses to the challenge of automated decision-making.

a. Governments should engage with their own sector-specific (insurance, credit reference agencies, banks, e-commerce sector) regulators to develop sector specific standards and guidelines to ensure that they are able to respond to the challenges of the use of algorithms in automated decision-making and taking into account the consumer interest.

b. Governments should consider to provide means of redress (complaint systems) to consumers who have been unfairly prejudiced by automated decision-making

c. Governments should ensure that consumers have access to key aspects of algorithms so that they are able to make informed decisions about which services to use.

d. Governments should make all automated decision-making systems used by any public authority or other government entity fully transparent and should provide all relevant information required for full scrutiny and auditing of such automated decision-making systems to all affected parties.

e. Governments should not engage in any actions which limits the ability to conduct research on, develop or understand automated decision-making systems.

f. Government should ensure that the individuals and organisations are held accountable for negligent use of automated decision-making systems.

g. Governments should ensure that free and fair elections remain possible

h. Governments should not impose a general obligation on Internet Intermediaries to use automated techniques to monitor information that they transmit or store.

i. Internet Intermediaries should be fully transparent with the users in the context of removal and blocking of content and should inform users whether and to what extent the decision-making in response to requests for taking down Internet content are automated or not.

j. Users should have the possibility to challenge the blocking and filtering of the content.

9. BIBLIOGRAPHY

Altonji, JG and RM Blank. 1999. 'Race and Gender in the Labor Market'. *Handbook of Labor Economics*. Retrieved (http://www.sciencedirect.com/science/article/pii/S1573446399300390).

Andreessen, Marc. 2011. 'Why Software Is Eating The World'. *Wall Street Journal*, August 20. Retrieved 1 September 2016 (http://www.wsj.com/articles/SB10001424053111903480904576512250915629460).

Article 29 Data Protection Working Party. 2013. *Opinion 03/2013 on Purpose Limitation*. Brussels, Belgium: ARTICLE 29 DATA PROTECTION WORKING PARTY. Retrieved (ARTICLE 29 DATA PROTECTION WORKING PARTY).

Asaro, Peter. 2013. 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making'. *International Review of the Red Cross* 94(886):687–709.

Bates, David W., Suchi Saria, Lucila Ohno-Machado, Anand Shah, and Gabriel Escobar. 2014. 'Big Data in Health Care: Using Analytics to Identify and Manage High-Risk and High-Cost Patients'. *Health Affairs* 33(7):1123–31.

Bertrand, Marianne and Sendhil Mullainathan. 2004. 'Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination'. *The American Economic Review* 94(4):991–1013.

Bijker, Wiebe E., Thomas P. Hughes, Trevor Pinch, and Deborah G. Douglas. 2012. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. MIT Press.

Bond, Robert M. et al. 2012. 'A 61-Million-Person Experiment in Social Influence and Political Mobilization'. *Nature* 489(7415):295–98.

Bozdag, Engin. 2013. 'Bias in Algorithmic Filtering and Personalization'. *Ethics and Information Technology* 15(3):209–27.

Bucher, Taina. 2012. 'Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook'. *New Media & Society* 1461444812440159.

Bucher, Taina. 2016. 'The Algorithmic Imaginary: Exploring the Ordinary Affects of Facebook Algorithms'. *Information, Communication & Society* 1–15.

Buni, Catherine and Soraya Chemaly. 2016. 'The Secret Rules of the Internet'. *The Verge*. Retrieved 9 September 2016 (http://www.theverge.com/2016/4/13/11387934/internet-moderator-history-youtube-facebook-reddit-censorship-free-speech).

Caliskan-Islam, Aylin, Joanna Bryson, and Arvind Narayanan. 2016. 'A Story of Discrimination and Unfairness Implicit Bias Embedded in Language Models Aylin'. in *Security & Privacy Week 2016*. Darmstadt; Germany: TU Darmstadt.

Chun, Wendy Hui Kyong. 2006. *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge Mass.: MIT Press.

Clay, Kelly. 2012. 'Is Microsoft Spying On SkyDrive Users?' *Forbes*. Retrieved 31 August 2016 (http://www.forbes.com/sites/kellyclay/2012/07/19/is-microsoft-spying-on-skydrive-users/).

Denardis, Laura. 2008. 'Architecting Civil Liberties'. in *Global Internet Governance Academic Network Annual Meeting*. Hyderabad (Andra Pradesh), India: GIGANET. Retrieved (http://worldcat.org/oclc/619234880/viewonline).

Denardis, Laura. 2012. 'Hidden Levers of Internet Control'. *Information, Communication & Society* (September):37–41.

Diakopoulos, Nicholas. 2015. 'Algorithmic Accountability'. *Digital Journalism* 3(3):398–415.

Elza Van Lingen. 2016. 'DA Refers Net1's Abuse of Advantage to Competition Commission'. *Democratic Alliance*. Retrieved 31 August 2016 (https://www.da.org.za/2016/02/da-refers-net1s-abuse-of-advantage-to-competition-commission/).

Ermert, Monika. 2013. *NSA-Abhörskandal PRISM: Internet-Austauschknoten Als Abhörziele*. Retrieved 19 August 2014 (http://www.heise.de/newsticker/meldung/NSA-Abhoerskandal-PRISM-Internet-Austauschknoten-als-Abhoerziele-1909604.html).
Gillespie, Tarleton. 2014. 'The Relevance of Algorithms'. Pp. 167–94 in *Media technologies: Essays on communication, materiality, and society*, edited by T. Gillespie, P. J. Boczkowski, and K. A. Foot. Cambridge Mass.: MIT Press.
Gillespie, Tarleton. 2016. 'Algorithm'. in *Digital Keywords: A Vocabulary of Information Society and Culture*, edited by B. Peters. Princeton University Press.
Goldin, Claudia and Cecilia Rouse. 1997. *Orchestrating Impartiality: The Impact of' Blind' Auditions on Female Musicians*. National bureau of economic research. Retrieved 9 September 2016 (http://www.nber.org/papers/w5903).
Goodman, Bryce and Seth Flaxman. 2016. 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"'. Retrieved (http://arxiv.org/abs/1606.08813).
Greenwald, Glenn and Ewen MacAskill. 2013. 'NSA Prism Program Taps in to User Data of Apple, Google and Others'. Retrieved (http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data).
Griffin, Andrew. 2016. 'How Facebook Is Manipulating You to Vote'. *The Independent*. Retrieved 31 August 2016 (http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-elections-2016-how-facebook-is-manipulating-you-to-vote-a7015196.html).
Heckert, Marc. 2011. 'Wie Ein Handy-Fan von Wolke Sieben Fiel'. *Aachener Zeitung*. Retrieved 31 August 2016 (http://www.aachener-zeitung.de/news/digital/wie-ein-handy-fan-von-wolke-sieben-fiel-1.372632).
Helberger, Natali. 2016. *Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law*. Rochester, NY: Social Science Research Network. Retrieved 31 August 2016 (http://papers.ssrn.com/abstract=2728717).
Helberger, Natali and Damian Trilling. 2016. 'Facebook Is a News Editor: The Real Issues to Be Concerned about'. *Media Policy Project*. Retrieved 9 September 2016 (http://blogs.lse.ac.uk/mediapolicyproject/2016/05/26/facebook-is-a-news-editor-the-real-issues-to-be-concerned-about/).
Hoofnagle, Chris Jay. 2003. 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement'. *NCJ Int'l L. & Com. Reg.* 29:595.
Irani, L. 2015. 'Difference and Dependence among Digital Workers: The Case of Amazon Mechanical Turk'. *South Atlantic Quarterly* 114(1):225–34.
Jędrzej Niklas, Karolina Sztandar-Sztanderska, and Katarzyna Szymielewicz. 2015. *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*. Warsaw, Poland: Panoptykon Foundation. Retrieved (https://en.panoptykon.org/articles/profiling-unemployed-poland-%E2%80%93-report).
Joerden, Jan C. 2015. 'Zum Einsatz von Algorithmen in Notstandslagen'. in *3. Würzburger Tagung zum Technikrecht*. Würzburg: Universität Würzburg.
Kaye, David. 2016. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to the Thirty-Second Session of the Human Rights Council*. Geneva, Switzerland.
Kirchner, Julia Angwin Surya Mattu, Jeff Larson, Lauren. 2016. 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks.' *ProPublica*. Retrieved 31 August 2016 (https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing).
Kitchin, R. and M. Dodge. 2011. *Code/space Software and Everyday Life*.
Kocher, Eva and Isabell Hensel. 2016. 'Herausforderungen Des Arbeitsrechts Durch Digitale Plattformen – Ein Neuer Koordinationsmodus von Erwerbsarbeit'. *Neue Zeitschrift Für Arbeitsrecht* (16/2016):984–89.
Kroll, Joshua A. et al. 2016. 'Accountable Algorithms'. Retrieved 1 September 2016 (http://balkin.blogspot.co.at/2016/03/accountable-algorithms.html).

Kroll, Joshua A. 2016. 'Accountable Algorithms (A Provocation)'. *Media Policy Project*. Retrieved 9 September 2016 (http://blogs.lse.ac.uk/mediapolicyproject/2016/02/10/accountable-algorithms-a-provocation/).
Lazer, David and Ryan Kennedy. 2015. *What We Can Learn from the Epic Failure of Google Flu Trends*.
Lazer, David, Ryan Kennedy, Gary King, and Alessandro Vespignani. 2014. 'The Parable of Google Flu: Traps in Big Data Analysis'. *Science* 343(6176):1203–5.
Lestrade, Niels. 2016. 'Use of Surveillance to Counter VERLT – Challenges and Opportunities to Safeguard Online Freedom'.
Lyon, David. 2003. 'Surveillance as Social Sorting: Computer Codes and Mobile Bodies'. in *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by D. Lyon. New York: Routledge.
Mantelero, Alessandro. 2016. 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection'. *Computer Law and Security Review* 32(2):238–55.
McCarthy, Daniel R. 2011. 'Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet'. *Foreign Policy Analysis* 7(1):89–111.
McIntyre, TJ. 2012. 'Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems'. in *Research Handbook on Governance of the Internet*, edited by I. Brown. Cheltenham: Edward Elgar.
Metz, Cade. 2008. *Phorm Secretly Tracked Americans Too*. Retrieved (http://www.theregister.co.uk/2008/08/13/phorm_us_tests/print.html).
Naughton, John. 2016. 'Digital Dominance: Forget the "digital" Bit'. *Media Policy Project*. Retrieved 9 September 2016 (http://blogs.lse.ac.uk/mediapolicyproject/2016/07/12/digital-dominance-forget-the-digital-bit/).
Nissenbaum, Helen. 2004. 'Privacy as Contextual Integrity'. *Wash. L. Rev.* 79:119.
O'Callaghan, D., D. Greene, M. Conway, J. Carthy, and P. Cunningham. 2014. 'Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems'. *Social Science Computer Review* 33(4):459–78.
Pariser, Eli. 2011. *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press.
Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
Perry, Walt L. 2013. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation. Retrieved 9 September 2016 (https://books.google.com/books?hl=en&lr=&id=ZdstAQAAQBAJ&oi=fnd&pg=PP1&dq=Perry,+Walter,+and+Brian+McInnis.+2013.+Predictive+Policing:+The+Role+of+Crime+Forecasting+in+Law+Enforcement+Operations.+Santa+Monica,+CA:+RAND.&ots=924yNa6Vct&sig=N3HnEi1FBr9YyMXV77GsgPbovYc).
Rifkind, Malcolm. 2014. *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby*.
Rosenblat, Alex, Tamara Kneese, and others. 2014. 'Networked Employment Discrimination'. *Open Society Foundations' Future of Work Commissioned Research Papers*. Retrieved 9 September 2016 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2543507).
Rosnay, Mélanie Dulong de. 2016. 'Algorithmic Transparency and Platform Loyalty or Fairness in the French Digital Republic Bill'. *Media Policy Project*. Retrieved 1 September 2016 (http://blogs.lse.ac.uk/mediapolicyproject/2016/04/22/algorithmic-transparency-and-platform-loyalty-or-fairness-in-the-french-digital-republic-bill/).
Rubinstein, Ira, Ronald D. Lee, and Paul M. Schwartz. 2008. *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*. Rochester, NY: Social Science Research Network. Retrieved 9 September 2016 (http://papers.ssrn.com/abstract=1116728).

Salamatian, Kavé. 2014. 'From Big Data to Banality of Evil'. Retrieved 9 September 2016 (https://www.oximity.com/article/Vortrag-Big-Data-und-Ethik-1).
Sills, Arthur J. 1970. 'Automated Data Processing and the Issue of Privacy'. *Seton Hall Law Review* 1.
Spiekermann, Sarah. 2015. *Ethical IT Innovation: A Value-Based System Design Approach*. CRC Press.
Staab, Steffen, Sophie Stalla-Bourdillon, and Laura Carmichael. 2016. 'Observing and Recommending from a Social Web with Biases'. *arXiv Preprint arXiv:1604.07180*. Retrieved 9 September 2016 (http://arxiv.org/abs/1604.07180).
Stanley, JE. 2011. 'Max Mosley and the English Right to Privacy'. *Wash. U. Global Stud. L. Rev.* 10(3). Retrieved (http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/wasglo10&section=25).
Steinbrück, Peer. 2012. *Vertrauen Zurückgewinnen: Ein Neuer Anlauf Zur Bändigung Der Finanzmärkte*. Berlin, Germany: Deutscher Bundestag - German Federal Parliament.
Tene, Omer and Jules Polonetsky. 2012. 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising'. Retrieved 9 September 2016 (http://conservancy.umn.edu/handle/11299/155947).
Tene, O. and J. Polonetsky. 2013. 'Judged by the Tin Man: Individual Rights in the Age of Big Data'. *J. on Telecomm. & High Tech. L.*
Toor, Amar. 2016. 'Automated Systems Fight ISIS Propaganda, but at What Cost?' *The Verge*. Retrieved 9 September 2016 (http://www.theverge.com/2016/9/6/12811680/isis-propaganda-algorithm-facebook-twitter-google).
Tufekci, Zeynep, Jillian C. York, Ben Wagner, and Frederike Kaltheuner. 2015. *The Ethics of Algorithms: From Radical Content to Self-Driving Cars*. Berlin, Germany: European University Viadrina. Retrieved (https://cihr.eu/publication-the-ethics-of-algorithms/).
Wagner, Ben. 2016a. 'Algorithmic Regulation and the Global Default: Shifting Norms in Internet Technology'. *Etikk I Praksis-Nordic Journal of Applied Ethics*.
Wagner, Ben. 2016b. *Global Free Expression: Governing the Boundaries of Internet Content*. Cham, Switzerland: Springer International Publishing.
Williams, Aime. 2016. 'How Facebook Can Affect Your Credit Score'. *Financial Times*, August 25. Retrieved 9 September 2016 (http://www.ft.com/cms/s/2/e8ccd7b8-6459-11e6-a08a-c7ac04ef00aa.html#axzz4JmmAbUyE).
Williams, Chris. 2008. *BT's Secret Phorm Trials: UK.gov Responds*. Retrieved (http://www.theregister.co.uk/2008/09/16/phorm_eu_berr/print.html).
Williamson, Ben. 2016. 'Computing Brains: Learning Algorithms and Neurocomputation in the Smart City'. *Information, Communication & Society* 0(0):1–19.
Winner, L. 1980. 'Do Artifacts Have Politics?' *Daedalus*.
Winner, L. 1986. 'The Whale and the Reactor: A Search for Limits in an Age of High Technology'.
Woolley, Richard, Charles Livingstone, Kevin Harrigan, and Angela Rintoul. 2013. 'House Edge: Hold Percentage and the Cost of EGM Gambling'. *International Gambling Studies* 13(3):388–402.
Yamamoto, Daisuke et al. 2014. 'Voice Interaction System with 3D-CG Virtual Agent for Stand-Alone Smartphones'. Pp. 323–30 in *Proceedings of the second international conference on Human-agent interaction*. ACM. Retrieved 31 August 2016 (http://dl.acm.org/citation.cfm?id=2658874).
York, Jillian C. 2010. 'Policing Content in the Quasi-Public Sphere'. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University.
Zhang, Pei, Sophie Stalla-Bourdillon, and Lester Gilbert. 2016. 'A Content-Linking-Context Model for "Notice-and-Take-down" Procedures'. Pp. 161–65 in. ACM Press. Retrieved 9 September 2016 (http://dl.acm.org/citation.cfm?doid=2908131.2908171).

Zuckerman, Ethan. 2013. *Digital Cosmopolitans: Why We Think the Internet Connects Us, Why It Doesn't, and How to Rewire It*. W. W. Norton & Company.
Zuiderveen Borgesius, Frederik J. et al. 2016. 'Should We Worry About Filter Bubbles?' *Internet Policy Review. Journal on Internet Regulation* 5(1). Retrieved 1 September 2016 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2758126).