Европейски парламент Parlamento Europeo Evropský parlament Europa-Parlamentet Europäisches Parlament
Euroopa Parlament Ευρωπαϊκό Κοινοβούλιο European Parliament Parlement européen Parlaimint na hEorpa
Europski parlament Parlamento europeo Eiropas Parlaments Europos Parlamentas Európai Parlament
Parlament Ewropew Europees Parlement Parlament Europejski Parlamento Europeu Parlamentul European
Európsky parlament Evropski parlament Euroopan parlamentti Europaparlamentet

Lista de publicaciones del Think Tank del PE

https://www.europarl.europa.eu/thinktank

Criterios de búsqueda a partir de los cuales se ha generado la lista :

Ordenar	Ordenar por fecha
Palabra clave	"cibernética"

15 Resultado(s) encontrado(s)

Fecha de creación : 18-04-2024

United States approach to artificial intelligence

Tipo de publicación: De un vistazo
Fecha: 17-01-2024
Autor: SZCZEPANSKI Marcin
Ámbito político: Protección de los consumidores
Palabra clave: América | ayuda a la reconversión | cambio tecnológico | cibernética | CIENCIA | ciencias naturales y aplicadas | ECONOMÍA | EDUCACIÓN Y COMUNICACIÓN | Estados Unidos | GEOGRAFÍA | geografía económica | geografía política | información y tratamiento de la información | inteligencia artificial | política económica | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | tecnología y reglamentación técnica
Resumen: While efforts to regulate artificial intelligence (AI) both globally and in the United States intensify, the prospects for broad Congress-passed legislation remain doubtful. In October 2023, President Biden issued a wide-reaching executive order on safe, secure and trustworthy AI. It is a positive step, but implementation will be challenging.
De un vistazo: EN

Dual-use and cyber-surveillance: EU policies and current practices

Tipo de publicación: Briefing
Fecha: 01-10-2023
Autor externo: Rudi Du Bois & Alexandre Tapia Reyes
Palabra clave: cibernética | CIENCIA | ciencias naturales y aplicadas | Derecho de la Unión Europea | reglamento (UE) | UNIÓN EUROPEA
Resumen: This briefing paper on dual-use and cyber-surveillance provides on overview of current EU export controls of dual-use items in general and cyber-surveillance items in particular, and what the approach is in countries such as the US, the UK and Japan. It explains the impact of the sanctions against Russia on the export of dual-use items and the use of cyber-surveillance in the conflict in the Ukraine.
The Dual-use Regulation 2021/821 has broadened the scope of export controls and defines a new category of dual-use items, namely 'cyber-surveillance items' which is incorporated in the list of dual-use items in Annex I of the Regulation. Further-more, the Regulation introduces a catch-all clause which makes the export of cyber-surveillance items not listed in Annex I subject to export authorisation when intended for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.
Regarding the sanctions against Russia, the EU had published 11 sanctions packages by mid-November 2023, including the prohibition of direct or indirect export to Russia of dual-use items listed in Annex I of the EU Dual-use Regulation. In addition, technologically advanced items as listed in Annex VII to the sanctions Regulation 833/2014 are also prohibited for export to Russia. The EU is cooperating with the US, the UK and other allies to align on the sanctions measures against Russia. There is less international alignment regarding export restrictions on semiconductor equipment and technology destined for China.
Briefing: EN

The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict

Tipo de publicación: Briefing
Fecha: 04-09-2023
Autor externo: Stéphane DUGUIN, Pavlina PAVLOVA
Ámbito político: Seguridad y defensa
Palabra clave: cibernética | CIENCIA | ciencias naturales y aplicadas | conflicto entre Rusia y Ucrania | construcción europea | Europa | GEOGRAFÍA | geografía económica | geografía política | guerra de información | política exterior y de seguridad común | RELACIONES INTERNACIONALES | Rusia | seguridad internacional | Ucrania | UNIÓN EUROPEA
Resumen: On 24 February 2022, the Russian Federation carried out a further military invasion of Ukraine, violating the UN Charter. The ongoing international armed conflict in Ukraine raises concerns about harm and impact caused to the civilian population, and the protection of civilians and civilian infrastructure which are affected by both kinetic and cyberattacks. This report analyses the magnitude of the cyber dimension of the war in Ukraine, its impact, and the lessons learned with the aim to increase understanding about the threat environment, and strengthen cyber resilience and defence capabilities across the EU and in neighbouring countries.
Briefing: EN

Artificial intelligence [What Think Tanks are thinking]

Tipo de publicación Briefing

Fecha 23-03-2023

Autor CESLUK-GRAJEWSKI Marcin

Ámbito político Industria | Política de investigación

Palabra clave análisis económico | cambio tecnológico | cibernética | CIENCIA | ciencias naturales y aplicadas | documentación | ECONOMÍA | EDUCACIÓN Y COMUNICACIÓN | estudio de impacto | información y tratamiento de la información | informática y tratamiento de datos | inteligencia artificial | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | publicación | seguridad informática | tecnología digital | tecnología y reglamentación técnica

Resumen The recent launches of artificial intelligence (AI) tools capable of generating direct textual answers to questions, notably the chatbot ChatGPT, and the development of general-purpose AI technologies, are expected to revolutionise the application of AI in society and the economy. New AI tools in general offer massive potential for developments in industry, agriculture, health, education and other areas. However, many scientists and politicians are calling for the establishment of a legal and ethical framework to avoid potentially detrimental impacts from the use of such technologies. The EU's approach to artificial intelligence centres on excellence and trust, aimed at boosting research and industrial capacity while ensuring safety and fundamental rights. In 2021, the European Commission proposed the AI Act to regulate this area, but that regulation is still being debated. According to European Parliament recommendations from May 2022, AI has huge potential to boost capital and labour productivity, innovation, growth and job creation. However, its development could also pave the way for potential mass surveillance and other detrimental impacts on fundamental rights and values. This note gathers links to the recent publications and commentaries from many international think tanks on artificial Intelligence.

Briefing EN

Strengthening cyber resilience

Tipo de publicación Briefing

Fecha 14-12-2022

Autor VIKOLAINEN Vera

Ámbito político Evaluación de impacto ex ante

Palabra clave cibernética | CIENCIA | ciencias naturales y aplicadas | construcción europea | contenido digital | criminalidad informática | Derecho de la Unión Europea | EDUCACIÓN Y COMUNICACIÓN | espacio de libertad, seguridad y justicia | informática y tratamiento de datos | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | reglamento (UE) | seguridad informática | tecnología y reglamentación técnica | UNIÓN EUROPEA

Resumen The present impact assessment (IA) accompanies the proposal for horizontal cybersecurity requirements for products with digital elements. The IA's strong points include a well-substantiated problem definition, an evidence base that appears to be recent and relevant, and a transparent account of the assumptions and limitations of the analysis. Furthermore, an effort has been made in the IA to quantify the total costs and benefits for the manufacturers of products with digital elements. However, the IA's analysis is predominantly economic, with little focus on environmental or social impacts. In addition to this, the general objectives set in the IA already appear rather prescriptive, leaving only two options that envisage horizontal requirements as real alternatives. Moreover, the IA has only partially reported on the stakeholder consultation activities, has not carried out a proper SME panel consultation, and did not explain why the open public consultation was reduced to 10 weeks.

Briefing EN

Europe's PegasusGate: Countering spyware abuse

Tipo de publicación Estudio

Fecha 06-07-2022

Autor MILDEBRATH Hendrik Alexander

Ámbito político Espacio de libertad, seguridad y justicia

Palabra clave cibernética | CIENCIA | ciencias naturales y aplicadas | comunicación | construcción europea | defensa | DERECHO | derechos y libertades | EDUCACIÓN Y COMUNICACIÓN | espacio de libertad, seguridad y justicia | espionaje | información y tratamiento de la información | informática y tratamiento de datos | medio de comunicación de masas | protección de datos | protección de las comunicaciones | RELACIONES INTERNACIONALES | seguridad informática | UNIÓN EUROPEA

Resumen As civil society and media organisations expose EU Member States for using the Pegasus commercial spyware, one of the most high-profile spying scandals of recent years is coming to light in Europe. Member States' intelligence agencies have been accused of abusing highly sophisticated spyware to surveil opposition figures, journalists, lawyers, and high-ranking state officials. 'Having regard to the European Union's attachment to the values and principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law', the European Parliament has set up a committee of inquiry. This study (i) introduces the Pegasus product's features and trading practices, (ii) surveys Pegasus operations and reactions, (iii) identifies transversal and country-specific legal concerns, and (iv) sketches possible ways forward in the public and private sectors.

Estudio EN

Pegasus and surveillance spyware

Tipo de publicación: Análisis en profundidad

Fecha: 06-05-2022

Autor: MARZOCCHI Ottavio | MAZZINI MARTINA

Ámbito político: Democracia en la UE, Derecho institucional y parlamentario | Espacio de libertad, seguridad y justicia

Palabra clave: cibernética | CIENCIA | ciencias naturales y aplicadas | comunicación | EDUCACIÓN Y COMUNICACIÓN | informática y tratamiento de datos | piratería informática | seguridad informática | software | transmisión de datos | tratamiento de datos

Resumen: This In-Depth Analysis, drafted by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs for the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, looks into the confirmed or suspected use of the Pegasus spyware and other similar cyber-surveillance instruments in the EU and its Member States or targeting EU citizens or residents, EU reactions and previous activities on issues related to surveillance.

Análisis en profundidad: EN

What if artificial intelligence in medical imaging could accelerate Covid-19 treatment?

Tipo de publicación: De un vistazo

Fecha: 21-12-2020

Autor: KRITIKOS Michail

Ámbito político: Derecho de la UE: sistema jurídico y actos legislativos | Empleo | Evaluación de la legislación y las políticas en la práctica | Mercado interior y unión aduanera | Planificación prospectiva | Política de investigación | Protección de los consumidores | Salud pública | Transporte

Palabra clave: ASUNTOS SOCIALES | cibernética | CIENCIA | ciencias naturales y aplicadas | diagnóstico médico | EDUCACIÓN Y COMUNICACIÓN | enfermedad por coronavirus | epidemia | información y tratamiento de la información | informática y tratamiento de datos | inteligencia artificial | material médico-quirúrgico | nueva tecnología | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | protección de datos | salud pública | sanidad | seguridad informática | tecnología y reglamentación técnica

Resumen: Thermal imaging cameras are currently being installed in office buildings, hospitals, shopping malls, schools and airports as a means of detecting people with fever-like symptoms. Given that these cameras are not necessarily designed to operate as medical devices, there are questions about their suitability in the context of the current pandemic. This note provides an overview of the use of thermal imaging empowered with artificial intelligence (AI) capabilities, its suitability in the context of the current pandemic and the core technical limitations of this technology. The main legal responses and ethical concerns related to the use of AI in the context of thermal imaging at entry points to identify and triage people who may have elevated temperatures are also examined.

De un vistazo: EN

What if blockchain could guarantee ethical AI?

Tipo de publicación: De un vistazo

Fecha: 21-12-2020

Autor: KRITIKOS Michail

Ámbito político: Asuntos financieros y bancarios | Derecho de la UE: sistema jurídico y actos legislativos | Medio ambiente | Planificación prospectiva | Protección de los consumidores | Salud pública | Seguridad alimentaria

Palabra clave: ASUNTOS FINANCIEROS | Banca electrónica | cadena de bloques | cibernética | CIENCIA | ciencias naturales y aplicadas | economía monetaria | EDUCACIÓN Y COMUNICACIÓN | humanidades | información y tratamiento de la información | informática y tratamiento de datos | instituciones financieras y de crédito | inteligencia artificial | libre circulación de capitales | mercado financiero | moneda virtual | nueva tecnología | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | protección de datos | seguridad informática | tecnología y reglamentación técnica | ética

Resumen: As artificial intelligence (AI) companies and other organisations are seeking ways to comply with ethical principles and requirements, blockchain, under specific circumstances, could be seen as a means to safeguard that AI is deployed in an ethically sound manner.

De un vistazo: EN

Multimedia: What if blockchain could guarantee ethical AI?

What if AI took care of traffic as well as driving?

Tipo de publicación: De un vistazo

Fecha: 21-12-2020

Autor: GARCIA HIGUERA ANDRES

Ámbito político: Industria | Planificación prospectiva | Política de investigación | Protección de los consumidores | Transporte

Palabra clave: cibernética | CIENCIA | ciencias naturales y aplicadas | comunicación | dispositivo de conducción | EDUCACIÓN Y COMUNICACIÓN | INDUSTRIA | industria del automóvil | industria mecánica | información y tratamiento de la información | informática y tratamiento de datos | inteligencia artificial | Internet de las cosas | nueva tecnología | organización de los transportes | política de transportes | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | seguridad en carretera | sistema de transporte inteligente | tecnología y reglamentación técnica | telemática | transporte por carretera | transporte terrestre | TRANSPORTES

Resumen: As happens with all applications of AI, autonomous vehicles require abundant data. Information external to the vehicle is crucial as it needs to know the structure of the road and the presence of obstacles or other vehicles in its path. Internal information is also essential, as the vehicle needs to know its own status and the reliability of critical elements, such as brakes. Even if autonomous vehicles need to detect traditional signals and allocate uncertainty areas while sharing the public thoroughfare with non-autonomous vehicles, pedestrians and even animals, an efficient exchange of information with as many other vehicles as possible will greatly increase, not only their performance but also their safety.

De un vistazo: EN

Multimedia: What if AI took care of traffic as well as driving?

What if AI could help us become 'greener'?

Tipo de publicación: De un vistazo

Fecha: 20-11-2020

Autor: KONONENKO Vadim

Ámbito político: Educación | Industria | Medio ambiente | Planificación prospectiva | Política de investigación | Protección de los consumidores | Salud pública | Transporte

Palabra clave: cambio tecnológico | cibernética | CIENCIA | ciencias naturales y aplicadas | construcción europea | desarrollo sostenible | ECONOMÍA | economía circular | economía verde | EDUCACIÓN Y COMUNICACIÓN | estrategia de crecimiento de la UE | información y tratamiento de la información | innovación | inteligencia artificial | investigación y propiedad intelectual | MEDIO AMBIENTE | nueva tecnología | política del medio ambiente | política económica | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | tecnología y reglamentación técnica | UNIÓN EUROPEA

Resumen: While some argue that AI can potentially be useful or even indispensable in ‘green transitions’, important questions remain open. Should AI be only used in resolving different specific problems (for example, intelligent pollinating robots replacing a declining bee population) or should AI be employed in ‘governing’ the sustainability of complex socio-economic systems such as mobility, food, and energy? While the latter option is currently technically unattainable and may be ethically dubious, it marks the axis of a political debate about possible synergies between sustainability and AI.

De un vistazo: EN

Multimedia: What if AI could help us become ‘greener’?

Un marco de la UE para la inteligencia artificial

Tipo de publicación: De un vistazo

Fecha: 14-10-2020

Autor: MADIEGA Tambiama André

Ámbito político: Derecho de la propiedad intelectual | Derecho de la UE: sistema jurídico y actos legislativos | Industria | Protección de los consumidores

Palabra clave: cambio tecnológico | cibernética | CIENCIA | ciencias naturales y aplicadas | DERECHO | Derecho civil | EDUCACIÓN Y COMUNICACIÓN | humanidades | impacto de la tecnología de la información | información y tratamiento de la información | informática y tratamiento de datos | inteligencia artificial | nueva tecnología | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | responsabilidad civil | robótica | seguridad informática | tecnología y reglamentación técnica | ética

Resumen: Los legisladores de la Unión Europea (UE) están reflexionando acerca de la mejor manera de legislar sobre el uso de la tecnología de inteligencia artificial (IA), intentando maximizar las oportunidades de que los ciudadanos de la UE se beneficien de esa tecnología y estableciendo, al mismo tiempo, normas contra sus riesgos. Está previsto que el Parlamento vote en su sesión plenaria de octubre II tres informes de propia iniciativa de la Comisión de Asuntos Jurídicos (JURI) en los ámbitos de la ética, la responsabilidad civil y la propiedad intelectual (PI).

De un vistazo: DE, EN, ES, FR, IT, PL

Perspectives on transatlantic cooperation: Transatlantic cyber-insecurity and cybercrime - Economic impact and future prospects

Tipo de publicación Estudio

Fecha 07-12-2017

Autor externo Benjamin C. Dean, Iconoclast Tech
Foreword by Patryk Pawlak, formerly of EPRS, now of EU Institute for Security Studies
Administrator responsible: Elena Lazarou, Members' Research Service, EPRS

Ámbito político Asuntos exteriores | Seguridad y defensa

Palabra clave atentado contra la seguridad del Estado | cibernética | CIENCIA | ciencias naturales y aplicadas | comunicación de datos | construcción europea | cooperación intergubernamental (UE) | criminalidad informática | DERECHO | Derecho penal | EDUCACIÓN Y COMUNICACIÓN | información y tratamiento de la información | informática y tratamiento de datos | política internacional | RELACIONES INTERNACIONALES | relación transatlántica | seguridad informática | seguridad pública | UNIÓN EUROPEA | VIDA POLÍTICA | vida política y seguridad pública

Resumen Over the past two decades, an 'open' internet and the spread of digital technologies have brought great economic benefits on both sides of the Atlantic. At the same time, the spread of insecure digital technologies has also enabled costly new forms of crime, and created systemic risks to transatlantic and national critical infrastructure, threatening economic growth and development. The transnational nature of these phenomena make it very difficult for effective policy solutions to be implemented unilaterally by any one jurisdiction. Cooperation between stakeholders in both the EU and US is required in the development and implementation of policies to increase the security of digital technologies and increase societal resilience to the cybersecurity risks associated with critical infrastructure. Although there is a great deal of congruence between the stated policy goals in both the EU and US, obstacles to effective cooperation impede effective transatlantic policy development and implementation in some areas. This study examines the scale of economic and societal benefits, costs, and losses associated with digital technologies. It provides an overview of the key cybercrime, cybersecurity and cyber-resilience issues that policy-makers on either side of the Atlantic could work together on, and explains where effective cooperation is sometimes impeded.

Estudio EN

Forward-looking policy-making at the European Parliament through scientific foresight

Tipo de publicación Briefing

Fecha 31-08-2017

Autor VAN WOENSEL Lieve

Ámbito político Planificación prospectiva | Política de investigación

Palabra clave análisis económico | cibernética | CIENCIA | ciencias naturales y aplicadas | documentación | ECONOMÍA | EDUCACIÓN Y COMUNICACIÓN | estudio de impacto | evaluación de conocimientos | humanidades | instituciones de la Unión Europea y función pública europea | organización de la enseñanza | parlamentario europeo | Parlamento Europeo | peritaje científico | UNIÓN EUROPEA | ética

Resumen The European Parliament's Science and Technology Options Assessment (STOA) Panel, supported by the Scientific Foresight Unit (STOA), decided two years ago to experiment with a process involving scenario development and assessment to explore possible future techno-scientific developments and their potential impacts, while backcasting possible future opportunities and concerns to options available to policy-makers today. This was achieved with the involvement of experts from a variety of backgrounds, together with stakeholders, using a multi-perspective approach. In this setting, various types of possible impacts are explored, which provide the foundations for imagined exploratory scenarios. From these scenarios we can learn about the possible challenges and opportunities arising from them. By communicating these challenges and opportunities to the Members of the European Parliament (MEPs), together with related legal and ethical reflections, the MEPs are provided with potential insights into how to anticipate future policy issues. The MEPs might thus be able to identify options for working towards the most desirable futures and avoiding undesirable futures, and even for anticipating undesirable scenarios. Therefore, foresight-based policy preparation can help the European Parliament stay well prepared for what might lie ahead, allowing informed, anticipatory action.

Briefing EN

Horizon scanning and analysis of techno-scientific trends: Scientific Foresight Study

Tipo de publicación Estudio

Fecha 05-07-2017

Autor externo Michael Baumgartner, Bijan Farsijani (Augmented Intelligence Institute; http://www.augmento.ai)

Ámbito político Planificación prospectiva | Política de investigación

Palabra clave biotecnología | cibernética | CIENCIA | ciencias naturales y aplicadas | comunicación | desinformación | EDUCACIÓN Y COMUNICACIÓN | genética | información y tratamiento de la información | informática y tratamiento de datos | inteligencia artificial | macrodatos | medios sociales | organización de los transportes | PRODUCCIÓN, TECNOLOGÍA E INVESTIGACIÓN | tecnología y reglamentación técnica | TRANSPORTES | vehículo eléctrico

Resumen This horizon scan has identified eight major technological trends relevant for STOA. First, a scan was conducted to measure controversy on social media, and this constituted an initial controversy ranking. After more detailed analysis of the main technology trends identified, a set of STOA-relevant areas were selected, which have not yet been investigated by STOA so far. These are big data, gene technology, electric vehicles, autonomous cars and impact of algorithms. A number of additional trend areas with high potential impact on society were identified for analysis: screen addiction, fake news and bioterrorism. Within the eight topics selected for detailed analysis from the initial horizon scanning process, keywords, subtopics, and sentiments have been detected and analysed from social media and news articles. These eight technologies are areas for discussion amongst the STOA Panel members when considering new project activities to be undertaken.

Estudio EN