Guía general para la realización de los trabajos

Las características del trabajo deben ser las siguientes:

a) La extensión de cada trabajo deberá ser de 4 a 6 folios, portada, índice y bibliografía no incluidos. Los trabajos deben presentarse impresos, no manuscritos, en letra Times New Roman, de cuerpo (tamaño) 12 con interlineado sencillo (a un espacio).
b) Deberán tener un índice.
c) Los trabajos comenzarán por una INTRODUCCIÓN donde se explicará brevemente la cuestión que se va a tratar.
d) Contarán con un ESTUDIO profundo de la situación, realizando un análisis actual, y recogiendo documentación (estadísticas, estudios, artículos, leyes, entrevistas…). De este análisis se deberán extraer una serie de conclusiones propias.
e) El alumno deberá exponer, como opinión personal, POSIBLES SOLUCIONES, dentro del marco de la Unión Europea, basadas en las conclusiones de su estudio.
f) Se debe incluir un apartado de BIBLIOGRAFÍA, donde se cite el material consultado para la elaboración del trabajo.

Hay que responder a las cuestiones formuladas en el planteamiento recogido en el primer párrafo del informe, para ello resultará útil pensar (se refleje o no en el trabajo, no hay por qué responder explícitamente a todas) sobre las cuestiones para la reflexión planteadas en el informe. Se debe realizar un análisis de los diferentes factores que influyen en la situación, intentando abarcar el mayor número de ámbitos posible (político, económico, medioambiental, sociológico, ético...). Es conveniente estudiar las principales corrientes de opinión sobre el tema, para adherirse, contradecir, o matizar estas posturas en el propio análisis. Se deberán apoyar las propuestas, en la medida de lo posible, con datos objetivos mostrados en el estudio (económicos, demográficos, legales...).

En ningún caso existe una respuesta "acertada" a las cuestiones, lo que valorarán los correctores es el estudio realizado de la materia y la coherencia entre éste y las propuestas presentadas al final del trabajo. Por supuesto las propuestas han de adecuarse a la realidad, además de al propio análisis, han de ser viables y realistas, y esto sí se valorará; pero no tendrá mejor puntuación un trabajo que plantee las propuestas de solución consideradas más acertadas por los correctores.

Documentación y citas

Se podrá utilizar la documentación aportada en los informes o cualquiera otra que se considere adecuada. En caso de duda sobre la fiabilidad de alguna fuente o un documento concreto se debe consultar con el profesor del propio centro o con el experto autor del informe a través del correo electrónico. Es siempre mejor consultar que utilizar documentación no fiable.

Es muy importante el correcto uso de la cita. Si se citan textos deben entrecomillarse y mencionar la fuente o procedencia. Asimismo si se recogen ideas de forma no textual, reelaborándolas, se deberá también citar la fuente. LA PRESENCIA DE FRAGMENTOS COPIADOS, SIN FORMATO DE CITA, PRESENTADOS COMO PROPIOS, SERÁ CONSIDERADA PLAGIO Y DESCALIFICARÁ EL TRABAJO.

Es recomendable apoyar nuestras afirmaciones en las fuentes, no es lo mismo decir que hay mucho paro, que dar el porcentaje exacto facilitado por Eurostat. Y lo mismo sucede con las ideas, no es lo mismo decir que algo es de determinada manera a secas, que recordar que tal estudio realizado por tal institución así lo dictamina, o que se está de acuerdo con las tesis de tal analista, político, u ONG.

No sólo es válido utilizar documentos ya existentes, es muy recomendable intentar buscar a alguien que sepa de la materia y plantearle nuestras preguntas. Sus respuestas nos ayudarán a entender mejor la cuestión, resolver dudas, y llegar a nuestras propias conclusiones. Esta persona no tiene por qué ser un experto de talla mundial, en cada localidad hay personas que se ocupan de la mayoría de los temas que se plantean (en Universidades, Ayuntamientos, o incluso en el propio centro). El profesor puede ayudar a encontrarlas. Pero esta entrevista debe ser una fuente de información más, lo más importante es la propia opinión, en ningún caso debe ser el trabajo sólo una entrevista.

Cuantas más fuentes y documentos se consulten mejor visión global se tendrá de las cuestiones, más completo resultará nuestro análisis, y mejor fundadas estarán las conclusiones. Esto no significa que debamos limitarnos a copiar los datos e ideas que encontremos, debe demostrase que se comprende la información y se encaja con otros datos o ideas. El trabajo debe ser personal, resultado de una reflexión individual y original sobre el tema.

Punto de vista

El Modelo de Parlamento Europeo es una oportunidad para ejercer de europarlamentario. Los trabajos deben por tanto reflejar una visión europea de las cuestiones. Se puede analizar el efecto que tal o cual política tendría para España, pero las propuestas han de ser lo que se considera mejor para toda la Unión Europea, y el análisis no puede estar limitado a un país sino que debe abarcar toda la UE.

Como representante de los ciudadanos, el parlamentario está obligado a escuchar todas las opiniones relevantes, analizarlas, valorarlas y realizar su propio estudio sobre las cuestiones. Y a proponer soluciones que beneficien a todos.

A continuación un informe específico sobre el tema. No es un modelo de cómo debe ser un trabajo, simplemente es una introducción al tema, y una orientación para comenzar el análisis propio. Al final se encuentran páginas de Internet útiles para recabar información, el nombre del experto y el correo electrónico donde dirigir las dudas. Se puede consultar cualquier duda sobre el trabajo, serán respondidas lo antes posible.

Comisión de Libertades Civiles, Justicia y Asuntos de Interior

La UE en la era digital

Introducción

Las tecnologías de la información están cambiando multitud de hábitos y procesos de una manera tan rápida y profunda que ni siquiera los escritores de ciencia ficción podían imaginar hace tan solo 50 años. Hoy en día es posible almacenar y enviar información en tiempo real alrededor del mundo con un coste muy pequeño, lo que supone una revolución en la economía, en el acceso al conocimiento e incluso en las relaciones personales.

Uno de los aspectos más preocupantes de la evolución de las nuevas tecnologías es que es muy difícil hacer previsiones sobre lo que va a venir en el futuro. Las posibilidades que brinda son tantas que solo se pueden hacer estimaciones en un plazo de menos de cinco años. El protagonismo de las redes sociales, la propagación mundial de los dispositivos móviles o la tecnología blockchain son fenómenos que no podían ser anticipados diez años antes de que sucedieran. El futuro nos depará inteligencia artificial, sensores por todas partes, realidad virtual, robótica y no sabemos qué cosas más. Ni tampoco cómo impactarán en nuestras vidas y en nuestras sociedades.

Economía de la colaboración

El desarrollo de internet ha traído nuevos modelos de negocio, en los que se reinventan las normas de juego de sectores tradicionales aprovechando las posibilidades de las tecnologías de la información y el grado de implantación entre los ciudadanos de las mismas. Así, por ejemplo, podemos poner nuestra casa en alquiler como particulares en tan solo unos minutos y alguien puede alquilarla desde el otro lado del mundo de manera sencilla y casi instantánea sin que haya habido una intervención humana de una tercera persona en el proceso. Del mismo modo podemos compartir un viaje en coche, pedir cualquier cosa a domicilio o alquilar diferentes tipos de vehículos por minutos.

La llamada economía de la colaboración está impactando positivamente en nuestras vidas ofreciéndonos nuevas posibilidades, pero también está generando algunos descontentos. Tanto en las empresas a las que hace competencia, como en ciudades donde incide en la subida de los precios de los alquileres o en la atracción de turistas ruidosos y poco considerados con los vecinos.

Además, en algunos casos las iniciativas de la *sharing economy* fomentan trabajos mal remunerados con fórmulas de contratación de falsos autónomos. Estos trabajadores ya comienzan a reivindicar judicialmente sus derechos laborales.

Nuevos delitos digitales

Con la implantación de las nuevas tecnologías no solo han aparecido nuevas formas de negocio, también han aparecido nuevas formas de delito o se han sofisticado las ya existentes. Los **estafadores** han encontrado un entorno sencillo de captar víctimas para sus fraudes. Así como también aquellos que se valen del supuesto anonimato de la red para insultar, **amenazar** o **calumniar**.

Se han creado nuevas unidades especializadas en delitos informáticos en los cuerpos de seguridad, pero todavía los ciudadanos se encuentran bastante indefensos, sobre todo en ausencia de formación específica para detectar los posibles timos o cómo proceder en caso de ser víctima de amenazas.

Darknet

En internet, como en el mundo no virtual, existen lugares ocultos donde se realizan actividades delictivas. Es el caso de la llamada *Darknet* (en algunos medios también conocida erróneamente como *Deepweb*) en la que se pueden vender y comprar drogas, armas y otras cosas ilegales. Sin embargo, más incluso que en la internet legal, los estafadores campan a sus anchas y lo más habitual si uno navega por esa internet oculta es encontrar ofertas de dudosa consideración.

La persecución de estas conductas es complicada porque se basan en tecnologías que permiten el anonimato. Sin embargo, las autoridades policiales y judiciales han conseguido importantes logros de cierre de sitios ilegales y captura de sus autores.

Protección de datos personales

Los riesgos asociados a la desprotección de nuestros datos personales son tales como su divulgación no autorizada, la suplantación de identidad y el abuso en línea (ciberacoso), entre otros muchos que no solemos imaginar como usuarios de la red.

Según datos de la Comisión Europea, actualmente 250 millones de personas utilizan internet cada día en Europa. Esto quiere decir que cada vez compartimos más datos personales, en operaciones tan cotidianas como la consulta de nuestros datos bancarios, compras por internet, comunicación por redes sociales o la presentación de declaraciones tributarias vía electrónica.

El pasado 25 de mayo de 2018 entró en vigor a nivel europeo el Reglamento general de protección de datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016). Así, a partir de ahora hay un único conjunto de normas de protección de datos para todas las empresas que operan en la Unión Europea (UE), con independencia de dónde tengan su sede, que protege el derecho fundamental de protección de datos de todos los ciudadanos de la UE.

Gracias a este cambio, las personas tienen más control sobre sus datos personales (aquellos relativos a una persona viva identificada o identificable, como son su nombre, apellidos, dirección, etc.) y las empresas se benefician de igualdad de condiciones.

Algunos de los derechos que quedan reconocidos a partir de ahora son los siguientes:

- **Derecho a recibir información clara y comprensible sobre quién trata sus datos**.
- **Derecho a solicitar acceso a los datos personales** que una organización tenga sobre ti.
- **Derecho a solicitar la "portabilidad de datos" de un servidor de internet a otro.**
- **El derecho a "ser olvidado" o derecho "al olvido"**: poder solicitar que se borren los datos personales si ya no desea que una empresa los trate.
- Obligación de las empresas de solicitar el **consentimiento expreso en el tratamiento de los datos personales de los ciudadanos.**
- **Mejor protección para los menores**.

Con esto, los ciudadanos tenemos mucha más información respecto a cómo son tratados nuestros datos y estamos más protegidos de cara a pedirles a las empresas que manejan nuestros datos, que los modifiquen o retiren de su base de datos.

Menores

La relación de los menores con la tecnología centra la preocupación en el denominado ciberacoso.

El bullying o acoso escolar es una manera de maltrato dentro del entorno escolar que se materializa en intimidación, aislamiento, insultos, amenazas,... buscando el daño físico o psíquico en la víctima. Ésta sufre así de baja autoestima, depresión, falta de integración, ansiedad, déficit de concentración en el estudio y hasta problemas de aprendizaje.

En este sentido el *cyberbullying* o ciberacoso es aquel que se realiza de manera repetida en el entorno virtual haciendo uso de ordenadores, smartphones o tablets, a través de redes sociales, email, Whatsapp o hasta en publicaciones en páginas web o blogs. A pesar de los esfuerzos de la Comisión Europea en esta temática, no existe una definición oficial de ciberacoso.

Los ataques suelen ir en forma de amenazas, publicaciones falsas, imágenes amenazadoras y pueden ir destinadas a una persona o a un grupo de personas. El acosador se suele esconder en identidades anónimas (también denominados *haters*) con el fin de proteger su identidad. A pesar de este supuesto anonimato, a diferencia del acoso tradicional, todas las acciones del acosador quedan registradas en la red siendo así fáciles de rastrear, sin necesidad de que la víctima tenga que testificar.

Con todo, pocos son los países que han tomado medidas para luchar contra el ciberacoso. En nuestro país, puede estar penado en el Código Penal como un ciberdelito o delito informático. Estos delitos son: delitos contra la intimidad, amenazas, la alteración o daños a datos de terceros, la pornografía infantil o los delitos contra el honor.

Las consecuencias en la víctima son similares a las del acoso escolar tradicional y se aprecian cuando la víctima comienza a perder el interés por asistir a los sitios donde considera que su acosador pueda estar (el colegio, determinados grupos de amigos, actividades extraescolares, etc.). El grupo de edad más afectado es el de adolescentes de entre 13 y 16 años, con más vulnerabilidad entre las chicas. La OMS señala que suelen sufrir acoso con más frecuencia los niños que proceden de familias más pobres.

Enfrentamiento virtual entre países de nuestro entorno

Con el auge, del mundo digital, se abre un nuevo campo de batalla entre los países.

Una de sus articulaciones pasa por la denominada **desinformación** o manipulación informativa. Ésta tiene como fin procurar a los destinatarios del mensaje de desconcierto e ignorancia y evitar asimismo la circulación de determinada información o datos desfavorables para el autor de esta acción. Se articula en la generación de noticias falsas (“fake news”), bulos, propaganda,... Si bien no se trata de una argucia militar nueva (ya se usaba en la Revolución Rusa), con el auge de la tecnología y la multiplicidad de canales de comunicación que ofrece Internet, su uso se extiende de manera incontrolada y forma parte de los enfrentamientos entre países.

Efectivamente, a través de redes sociales y medios de comunicación nuevos, se crean contenidos que tienen como fin conseguir determinadas acciones que favorezcan a unos u otros. De hecho, se considera que la desinformación está teniendo una gran influencia en los procesos democráticos de los últimos tiempos.

A principios de este año el presidente francés, Macron, apeló por una legislación específica para combatir la sistemática propagación de la intoxicación informativa con fines políticos. Este debate, sin embargo, se articula complicado dado que puede chocar con el **derecho fundamental de libertad de expresión**. La Comisión Europea hizo reciente sus deberes en esta materia con la realización del estudio “Un enfoque multidisciplinar a la desinformación”, que destacó como puntos para trabajar en este tema, entre otros, los siguientes: un rechazo a la censura de contenidos, una llamada a contrarrestar la injerencia de determinada información con las elecciones, un compromiso de las plataformas a compartir determinados datos, un llamamiento a hacer mayores esfuerzos en la alfabetización digital y un esfuerzo de todos los países de la UE en la evaluación e impacto de la desinformación.

Otro enfrentamiento entre países a través de la tecnología es el de los **ciberataques**. Un ciberataque es aquella operación ofensiva que tiene como fin atacar un sistema operativo

tecnológico tales como bases de datos, sistemas operativos, ordenadores, etc. por medio de actos originados en fuentes anónimas. El objetivo de estos ataques suele ser robar, borrar o alterar el contenido de determinada información o manipular ciertos contenidos.

En el contexto del sabotaje y el espionaje, se denomina **Guerra cibernética** a aquellos ciberataques controlados por los Gobiernos que tienen como fin enfrentarse para lograr un determinado objetivo cuyos militares son los denominados *hackers*.

Además de los conocidos virus informáticos, los ataques que más aumentado en los últimos años son el envío de gran cantidad de llamadas de forma simultánea a un único servidor, que exceden su capacidad de respuesta y consiguen así paralizarlo; son los llamados ataques de denegación de servicio (DDoS).

Cuestiones para iniciar la reflexión

A la luz de la información anterior y vistos los posibles peligros que existen dentro de Internet, vamos a reflexionar sobre cómo actuar de manera consciente en la red.

- ¿Crees que en los próximos años el smartphone seguirá siendo el principal dispositivo para acceder a Internet?
- ¿Crees que deberían limitarse las actividades de la sharing economy? ¿Qué retos plantea a nivel de libertades individuales?
- ¿Cómo crees que pueden prevenirse delitos digitales como la estafa online o las amenazas en redes sociales?
- ¿Qué esfuerzos se podrían llevar a cabo a nivel europeo para luchar contra las actividades de la *darknet*?
- ¿Sabes lo que es tu huella digital y cómo puede ser usada por terceros sin tu conocimiento?
- ¿Crees que los ciudadanos estamos desprotegidos respecto al manejo de información que determinadas empresas disponen de nosotros?
- ¿Crees que este manejo te ofrece beneficios o que te puede llegar a afectar negativamente en un determinado momento?
- Respecto a las últimas filtraciones de datos de usuarios de Facebook, ¿cuál crees que es la responsabilidad que las grandes empresas tecnológicas deberían asumir?
- ¿Cuáles son las garantías mínimas que las grandes plataformas tecnológicas deberían dar a sus usuarios?
- ¿Cómo pueden ayudar los países en materia de legislación para que las grandes empresas puedan proteger los datos de sus usuarios?
- A la vista de la era de la desinformación y la postverdad, ¿crees que los medios de comunicación tradicionales son fiables?
- ¿Cómo podemos hacer los ciudadanos para contrastar las noticias que nos vienen dadas como verídicas y no dejarnos afectar por ellas en decisiones importantes que afectan nuestro entorno, como en cuestiones democráticas?

- ¿Cómo crees que te afecta personalmente como ciudadano los ciberataques entre países?
- ¿Has presenciado como usuario de una red social alguna vez un ciberacoso?
- ¿Cuál es el rol que debería tener un usuario que presencia un ciberacoso en la red?

Documentación

Los cambios tecnológicos que transformarán la sociedad la próxima década
http://www.lavanguardia.com/vida/20180123/44225498552/cambios-sociales-tecnologia-predicciones-proxima-decada.html

BlaBlaCar es legal: la plataforma de compartir gastos de transporte gana el juicio a Confebus
http://www.expansion.com/juridico/opinion/2017/02/03/58947b5e268e3e690d8b45a0.html

Deliveroo afronta su primer juicio en Barcelona por el despido de un repartidor
https://elpais.com/economia/2018/05/22/actualidad/1526999046_364771.html

¿Qué le está pasando a Airbnb en España?
https://hipertextual.com/2017/06/problemas-en-airbnb

El protocolo a seguir ante las injurias y las amenazas en internet
https://www.elconfidencial.com/tecnologia/2014-11-14/el-protocolo-a-seguir-ante-las-injurias-y-las-amenazas-en-internet_454488/

Viaje al lado oscuro de internet
http://www.elmundo.es/espana/2015/03/05/54f7513cca47413e0f8b4570.html

Así cayeron AlphaBay y Hansa, las sucesoras de Silk Road que dominaban la venta de productos ilegales en la Dark Web
https://www.xataka.com/legislacion-y-derechos/asi-cayeron-alphabay-y-hansa-las-sucesoras-de-silk-road-que-dominaban-la-venta-de-productos-ilegales-en-la-dark-web

Atacar la desinformación
https://elpais.com/elpais/2018/01/04/opinion/1515081755_445703.html

Seis puntos clave del informe sobre desinformación del Grupo de expertos de la Comisión Europea
https://www.eldiario.es/tecnologia/desinformacion-Grupo-expertos-Comision-Europea_0_749275859.html

España figura entre los países donde más ciberacoso sufren los menores
https://www.efe.com/efe/espana/sociedad/espana-figura-entre-los-paises-donde-mas-ciberacoso-sufren-menores/10004-2868427

Ciberacoso
https://es.wikipedia.org/wiki/Ciberacoso

Bullying o acoso escolar
http://europa.eu/youth/es/article/66/4888_es

Normas sobre protección de datos personales dentro y fuera de la UE
https://ec.europa.eu/info/law/law-topic/data-protection_es

Contacto

El presente informe ha sido elaborado por Ignacio Sevilla Priestley, periodista, se pueden plantear preguntas sobre el tema en la dirección de correo electrónico info@modeloparlamentoeuropeo.org