Enginyeria de Programari

Grau en Enginyeria Informàtica

Escola Politècnica Superior

Universitat de Lleida

Enunciado de Práctica – CURSO 23/24

Plataforma accesible de Gestión Ciudadana con reconocimiento biométrico

Tras casi dos años de la famosa campaña '*Soy mayor, no idiota*', impulsada por Carlos San Juan, un hombre de 78 años, para pedir un trato más humano en las sucursales bancarias en una lucha contra la exclusión financiera de los mayores, ha llegado el momento de hacer balance. A pesar de que se han conseguido algunos logros (mantener vigentes las libretas bancarias para los mayores de 65 años, así como otras medidas dentro del protocolo de buenas prácticas de la banca), resultan insuficientes. Además, este tipo de medidas son voluntarias, y por ello se reclama que se conviertan en ley. Otro problema primordial es que no se ha reducido la complejidad de los cajeros ni de las aplicaciones, lo cual es un claro indicador de que sigue existiendo una brecha digital.

Por otro lado, es evidente que este tipo de problemática no afecta únicamente a la banca. Hoy en día las administraciones públicas del estado (en lo sucesivo AAPP, tal como la Seguridad Social o la Dirección General de Tráfico) ofrecen numerosas facilidades para la realización de trámites de manera telemática. Gracias a ello, los ciudadanos pueden consultar datos de carácter personal y acceder a diferentes servicios disponibles online. De nuevo, las persones mayores se quedan al margen de todos estos avances. Se requiere un paso de registro en uno o varios sistemas de identificación en distintos organismos oficiales, así como gestionar certificados o claves digitales, los cuales son complejos de manejar y de recordar, sin olvidar que las contraseñas van caducando periódicamente. No hay que descuidar, por otro lado, la posibilidad de fraudes relacionados con el robo y suplantación de la identidad.

La plataforma propuesta aquí surge con la idea de facilitar a toda la ciudadanía acceso automático no sólo a servicios bancarios básicos y distintos trámites administrativos, sino también utilizar esa misma infraestructura para ofrecer acceso a un sistema de voto electrónico en periodos electorales. Todo ello eludiendo los pasos de registro y autenticación mediante clave o certificado, que suelen convertirse en una pesadilla para las personas mayores. Para ello se valdrá de la información biométrica que viene incrustada en los *pasaportes electrónicos*[1] vigentes hoy en día.

El sistema hará uso de una infraestructura similar a la existente en algunos aeropuertos (e.g. el del Prat de Llobregat). Se trata de *terminales de verificación de documentación*[2], específicamente preparados para el procesamiento automático de datos biométricos. En particular, procesan la imagen facial y la huella digital, datos que incorporan los pasaportes electrónicos. Este tipo de terminal está provisto de los siguientes periféricos: lector de pasaporte electrónico, lector

[1] El pasaporte electrónico español incorpora, siguiendo la norma ICAO, un chip RFID embebido en su portada trasera, que es capaz de identificar a sus titulares. El chip almacena de forma segura datos biométricos relativos a la imagen facial y a la huella digital del titular, así como los datos personales incluidos en las líneas OCR (Optical Character Recognition) (https://www.dnielectronico.es/portaldnie/PRF1_Cons02.action?pag=REF_1080). Actualmente coexisten en España dos modelos de pasaporte electrónico, expidiéndose desde el año 2015 únicamente el modelo 3.0 en todas las oficinas y equipos de expedición.

[2] Ordenador específicamente concebido para la identificación automática y verificación de documentos, provisto del software y hardware de biometría de la imagen facial y de la huella digital (https://www.abc.es/sociedad/abci-como-pasar-control-pasaporte-20-segundos-201707262155_noticia.html).

biométrico de reconocimiento facial[3] y lector de huella digital. Adicionalmente, con el propósito de ampliar sus funcionalidades a las descritas aquí, serán provistos de un lector de libretas bancarias universal, pantalla táctil y teclado alfanumérico para la interacción con el usuario.

Aunque se prevé comenzar con una prueba piloto en determinadas ciudades del país, la idea es poner a disposición del ciudadano toda esta infraestructura en los espacios comúnmente habilitados como colegios electorales en los distintos distritos de cada municipio. El número de terminales dependerá de varios factores, entre ellos el espacio disponible y el número de habitantes de cada municipio.

A. Verificación biométrica de la identidad del usuario

La verificación biométrica consiste en comprobar que el usuario es quien dice ser, y que acredita a través de un documento de identidad especialmente habilitado con parámetros biométricos, como es el caso del pasaporte electrónico hoy en día. Para ello es necesario disponer de la infraestructura adecuada, anteriormente descrita.

Este proceso consta de dos partes:

1) *Comprobación de los datos biométricos relativos a la imagen facial*. El usuario coloca el pasaporte en el lector de pasaporte electrónico, lo que permite proceder a su lectura. Lo primero que comprueba el sistema es la validez del documento. Si es correcto, el usuario se sitúa frente al terminal para enfocar la mirada a la cámara frontal. Esto permite capturar los datos biométricos de la cara. Éstos serán contrastados con los registrados en el pasaporte, como primer paso de la comprobación biométrica.

Por supuesto, todos los pasos van siendo indicados oportunamente por el sistema.

2) *Comprobación de los datos biométricos relativos a la huella digital*. A continuación, el usuario sitúa el dedo para proceder a la lectura de la huella digital, a contrastar también con la del pasaporte.

Se trata de un doble mecanismo de comprobación biométrica, a fin de aportar mayor seguridad. Sólo en caso de que todo sea validado correctamente y se verifique la identidad del usuario, la operativa del sistema sigue adelante. En caso contrario se informa al usuario y la sesión finaliza.

Por otro lado, a fin de dar respuesta al Reglamento General europeo de Protección de Datos[4] (RGPD), el uso del sistema aquí descrito requiere informar con claridad al usuario de la necesidad de capturar ciertos datos biométricos, así como de la finalidad con la que éstos se obtienen. Es por ello que, previo a la obtención de los parámetros biométricos, el sistema deberá solicitar consentimiento explícito al usuario. Sólo si es otorgado se procederá a la verificación biométrica.

Cabe señalar que la mayoría de las funcionalidades del sistema están preparadas para verificar la identidad del usuario únicamente mediante reconocimiento biométrico. Sin embargo, para el caso del sistema de voto electrónico el votante escogerá entre verificación manual o biométrica. Para ello, a lo largo de la jornada electoral se contará con personal de soporte, quien se encargará de verificar la identidad de manera manual (mediante uso del DNI), cuando así se requiera. Ambos procesos de identificación se detallan a continuación.

B. Servicios ofrecidos

La estructura básica del sistema consistirá en una primera pantalla, a fin de escoger, por parte del usuario, entre tres grandes apartados: operativa bancaria, trámites administrativos y sistema de voto electrónico (periodos electorales).

---

[3] Sistema de reconocimiento que utiliza dos cámaras para capturar los puntos biométricos del rostro, proporcionando una plantilla biométrica que sirve para identificar al individuo. La extracción de esta información implica sofisticados procesos matemáticos y algoritmos de coincidencia.

[4] Entró en vigor en mayo del 2018 con el anteproyecto de la nueva Ley Orgánica de Protección de Datos 2018 (https://ayudaleyprotecciondatos.es/2017/06/27/lopd-2018/#Articulo_9Tratamiento_de_datos_amparado_por_la_ley).

Adicionalmente, se ofrecerá una herramienta de ayuda de última generación cuya misión es ofrecer instrucciones claras y concisas vía voz ante cualquier duda o consulta relativa a la operativa del sistema. Se trata de un módulo de inteligencia artificial basado en reconocimiento de voz, a fin de facilitar la interacción con el sistema en cualquier momento durante la realización de cualquier gestión. Estará siempre al alcance del usuario (tecla o botón específico), por lo que podrá ser invocado en cualquier momento, a fin de ofrecer orientación específica. Asimismo, será capaz de actuar automáticamente en aquellos casos en que se detecte en el usuario un patrón de interacción errático o indicativo de confusión, con el propósito de sugerirle algún tipo de ayuda o recomendación.

Por supuesto, en ocasiones no se podrá ofrecer una respuesta concisa (la cuestión planteada no le resulta conocida al sistema, el trámite consultado no está disponible, o no se ha comprendido el mensaje del usuario, entre otros), en cuyo caso será comunicado al usuario, igualmente vía voz, acompañada de algún tipo de sugerencia.

A continuación, se presentan en detalle cada uno de los servicios ofrecidos.

1. Sistema de voto electrónico

Un sistema de voto electrónico es aquel que utiliza medios y tecnologías digitales en todas las fases del ejercicio del derecho al voto. Adecuadamente diseñadas, las soluciones de voto electrónico tienen fortalezas destacadas, como son la agilidad, la reducción en los costes y la universalidad. Sin embargo, sigue planteando retos importantes, especialmente de carácter social, como es la desconfianza ante la posibilidad de fraude.

A continuación se detalla el sistema de voto electrónico a desarrollar.

A) Tipo de sistema de voto electrónico escogido

Se está interesado en implantar, dentro de la modalidad de voto presencial[5], la tipología de *registro electrónico directo*, en la que una vez emitido el voto, éste no es transmitido a través de internet al centro de cómputo autonómico, sino que es escrutado[6] localmente (vía red local habilitada en el propio colegio electoral). No es hasta que concluye la jornada electoral que el escrutinio resultante se transmite al centro de cómputo autonómico.

La implantación del control automático de la identidad de los votantes[7] a través de la biometría[8] introduce un mayor grado de automatización en el proceso, sin comprometer la libertad en el ejercicio del derecho al voto, velando contra la posibilidad de suplantación de la identidad.

Ahora bien, dado que no todo el mundo dispone de pasaporte, o bien en los casos en que el usuario opte por no ceder sus datos biométricos denegando el consentimiento explícito, se podrá optar por ejercer el derecho al voto mediante el DNI. Utilizar uno u otro documento de identidad comporta diferencias únicamente en el paso de identificación, las cuales se indican a continuación.

B) Infraestructura hardware y recursos humanos

Además de los terminales de verificación, que en este contexto actuarán como terminales de voto, cabe contar también con los siguientes recursos en cada colegio electoral:

- *Recursos humanos*. En caso de elecciones los votantes contarán con el apoyo de personal especializado para garantizar el buen funcionamiento y seguimiento de la jornada electoral.

[5] No se trata de un sistema de voto en línea, lo que obliga a ejercer el derecho al voto en locales o colegios electorales físicos, controlados por el organismo electoral competente.

[6] Escrutar: reconocer y computar los votos, incorporando los votos emitidos en el recuento de votos ya escrutados.

[7] Ciudadano que figura en el censo electoral (en nuestro caso un censo electrónico), independientemente de si éste acaba ejerciendo su derecho al voto o no.

[8] Tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, constituyendo un sistema de identificación que aporta seguridad y comodidad.

Como ya se ha mencionado, entre otras cosas, se encargarán de realizar manualmente los pasos de *verificación de la identidad del votante* y también de *verificación del derecho al voto* en los casos en que no vaya a desplegarse la biometría (los dos casos mencionados arriba). El personal de soporte deberá resolver el paso de autenticación ante cualquier tipo de operación. El número de miembros de personal de soporte será proporcional a la cantidad de terminales disponibles en cada colegio electoral.

- *Servidor local*. Cada colegio electoral contará con un servidor local. Su operativa es esencial para el buen funcionamiento del sistema, pues centraliza la red local que interconecta los diferentes terminales de voto. En concreto, se encarga de gestionar tres piezas clave del proceso: 1) el escrutinio de los votos; 2) las cuentas de acceso del personal de soporte, a validar en el paso de autenticación; y 3) la conexión con los servicios externos, tal y como se explica más adelante.

A continuación, se presenta la funcionalidad que deben cubrir los terminales durante el ejercicio del voto.

C) Funcionalidad asociada a los Terminales de Voto

A continuación, se relacionan los pasos necesarios para *ejercer el derecho al voto* por parte de la ciudadanía.

1. *Indicar tipo de documento de identidad a utilizar*. Antes de iniciar la sesión de voto, el votante debe indicar qué documento de identidad aporta. En caso de aportar el DNI, el sistema informa que se necesita la intervención de personal de soporte y muestra pantalla de autenticación. En caso de aportar pasaporte electrónico se lleva a cabo el paso *2.* descrito a continuación.
2. *Solicitar el consentimiento explícito para el uso de datos biométricos*, en caso de aportar el pasaporte electrónico, tal y como ya se ha mencionado anteriormente.

   En caso de otorgar su consentimiento se aplicará el proceso automático de verificación biométrica haciendo uso del pasaporte electrónico. Caso de denegarlo, el votante podrá seguir el proceso manual, mediante el uso del DNI. La operativa a seguir en ambos casos se describe a continuación.
3. *Verificar identidad del votante*. Consiste en comprobar que el votante es quien dice ser, y que acredita a través de su documento de identidad. En este caso hay que tener en cuenta las dos situaciones mencionadas:

   Caso A: proceso automático. Se trata del proceso de identificación descrito anteriormente (sección *Verificación biométrica de la identidad del usuario*).

   Caso B: proceso manual. El votante aporta el DNI. En este caso será el personal de soporte quien compruebe de la manera tradicional la identidad del votante, esto es, verificando que dicha persona es la que aparece en la foto. Igualmente, es necesario verificar la validez del DNI.

   Si todo es correcto, el personal de soporte tecleará el NIF, quedando así verificada la identidad del votante, y todo a punto para verificar el derecho al voto (paso *4.* siguiente).

   En caso contrario, el ciudadano no podrá ejercer el derecho al voto y deberá abandonar el colegio electoral. La sesión de voto finaliza y el sistema vuelve a la pantalla de inicio.
4. *Verificar el derecho al voto*. Consiste en comprobar que todas las circunstancias son adecuadas para poder ejercer el derecho al voto (el votante consta en el censo electoral y aún no ha ejercido el derecho al voto). Para ello se requiere la obtención del NIF.

Igual que en el paso anterior, la obtención del NIF podrá ser realizada automáticamente cuando el votante aporte el pasaporte electrónico (aplicando técnicas de OCR[9], o bien leyendo del chip incrustado). En caso contrario se introduce manualmente por parte del personal de soporte, tal y como ya se ha mencionado en el paso *3*. anterior.

En cualquier caso, tras obtener el NIF, el sistema se conecta al organismo electoral para lanzar la consulta. Éste devolverá una respuesta favorable si todo es correcto, o desfavorable si alguna cosa no se cumple.

5. *Emitir el voto*. Una vez superados todos los pasos de verificación, se despliegan los menús y/o sistemas de navegación diseñados específicamente para las elecciones en curso. El votante navegará tantas veces como lo necesite por la interfaz para seleccionar adecuadamente su opción de voto[10]. A continuación, ésta se muestra en pantalla, a la espera de confirmación por parte del votante.

   Tan pronto es confirmado, el sistema procede a escrutar el voto emitido, incorporándose al recuento de votos a nivel de colegio electoral, vía transmisión al servidor local.

   Además, el sistema vuelve a conectarse al organismo electoral para registrar en el censo que el votante ya ha ejercido su derecho al voto. De esta forma queda inhabilitado para el ejercicio del voto en estos comicios, evitando así la posibilidad de duplicación del voto.

6. *Cerrar sesión*. Por último, la sesión de voto finaliza y el terminal de voto presenta de nuevo la pantalla de inicio.

Todos los pasos preparatorios previos a la jornada electoral (e.g. verificación del estado del censo electrónico e inicialización del recuento de votos a nivel local, entre otros), así como los pasos posteriores, entre ellos transmitir al centro de cómputo autonómico los datos resultantes del escrutinio a nivel de colegio electoral, serán obviados por simplicidad.

2. Operativa bancaria básica

A pesar de que mantener vigentes las libretas bancarias para los mayores de 65 años es uno de los acuerdos conseguidos por parte de la banca tras las reivindicaciones de las plataformas de mayores, es cada vez más evidente que están sufriendo un proceso de retroceso. Prueba de ello es que los diseños futuristas de cajeros automáticos tienden a eliminar el lector de libretas, obligando a los usuarios a pasar por ventanilla, sin olvidar que numerosas entidades bancarias están dejando de emitirlas. Con objeto de intentar paliar esta discriminación, se propone incluir también en la plataforma propuesta un servicio básico para libretas bancarias, el cual se describe a continuación.

Lectura y actualización de libretas bancarias

Los terminales descritos vendrán provistos de un lector de libretas bancarias universal, con el propósito de habilitar la realización de operaciones bancarias básicas, en independencia de la entidad bancaria. En este apartado, pensando específicamente en los clientes sénior, la interfaz deberá ser especialmente simple, adecuada a las personas menos familiarizadas con las nuevas tecnologías, mediante un diseño adaptado y una tipografía de mayor tamaño.

Para ello, una vez el usuario se ha identificado mediante el sistema biométrico, y tras seleccionar la sección de operativa bancaria, podrá realizar los siguientes pasos:

1. Introducir la libreta en el lector de libretas bancarias.

[9] Tecnología consistente en identificar automáticamente símbolos o caracteres que pertenecen a un determinado alfabeto, a partir de una imagen para ser tratados como datos.

[10] Se refiere a las opciones de voto existentes, entre las que elegir, las cuales son específicas de una determinada jornada electoral. Las opciones de voto incluyen también el voto en blanco y el voto nulo –a considerar en el sistema como una opción de voto adicional.

2. Introducir el Número de Identificación Personal (PIN) de la libreta (el hecho de estar identificado en el sistema no exime de haber de conocer el código de acceso a la libreta bancaria). Se descartan sistemas más modernos, como la biometría facial o vocal, pues tan sólo una minoría de las libretas bancaras están habilitadas con datos biométricos, además de la posibilidad de suplantación de la voz. Se opta, por tanto, por el sistema tradicional a través del PIN.
3. A continuación, el sistema detecta si existen movimientos pendientes. Indicará la posibilidad de actualizar la libreta, o bien dará a conocer que la libreta está actualizada.
   Se procederá a la actualización de la libreta únicamente si el usuario así lo indica.
   Es necesario contemplar la posibilidad de que la libreta puede agotarse antes de finalizar el proceso de actualización. En ese caso el sistema lo indicará en pantalla y extraerá automáticamente la libreta.
   Otra característica a incorporar es la de ofrecer la posibilidad de cancelar el proceso de actualización en cualquier momento por parte del usuario. El sistema detiene el proceso hasta indicación de reanudación del mismo, o bien de extracción de la libreta.
4. Una vez finalizada la actualización, la libreta permanecerá insertada. Se procederá a su extracción cuando el usuario así lo indique.

3. Gestión de trámites administrativos

Dado que nos encontramos en una primera fase de implantación, se propone comenzar habilitando un solo servicio asociado a las AAPP: la solicitud del certificado de nacimiento.

Los trámites ofrecidos ser irán ampliando paulatinamente en posteriores fases de implantación.

Solicitar el certificado de nacimiento

Como es popularmente conocido, el certificado de nacimiento es un documento expedido por el registro civil o consulado correspondiente, quien da fe del hecho del nacimiento, fecha y hora en que tuvo lugar, así como los datos de identidad del inscrito. Este documento es requerido para realizar numerosos trámites (una boda, solicitar el DNI, solicitar prestaciones económicas, etc.).

Una vez el usuario se ha identificado mediante el sistema biométrico, y tras seleccionar la sección de trámites administrativos, podrá realizar los siguientes pasos:

1. Seleccionar la subsección registro civil, y una vez allí el trámite ‘certificado de nacimiento’.
2. El sistema generará una copia del certificado, que se presentará en una nueva pestaña en formato pdf.
3. Desde allí tan sólo quedará dar el paso de descargarlo y/o de imprimirlo.

En ocasiones, la inscripción de nacimiento solicitada no consta en la información disponible por el registro civil local. Esto puede ser debido a que el registro civil en el que está inscrita esa persona pertenece a otra provincia, comunidad autónoma o país.

En estos casos se requieren ciertos pasos adicionales en los que el usuario deberá intervenir. Se trata de los siguientes pasos: 1) rellenar un formulario con datos personales; y 2) dar la conformidad para realizar la solicitud; para finalmente 3) generar el certificado por parte del sistema. Igualmente, el usuario podrá optar por descargar y/o imprimir el certificado.

C. Restricciones y propiedades a cumplir por el sistema

A continuación, se relacionan las restricciones y propiedades que debe cumplir el sistema con el fin de ofrecer garantías suficientes para su implantación. Buena parte de ellas están asociadas específicamente al sistema de voto electrónico.

a) En primer lugar, y como más importante, debe garantizarse el cumplimiento de los principios electorales propios de cualquier sistema de votación. En síntesis son: garantía de

fiabilidad y seguridad, universalidad[11], igualdad[12], así como que el derecho al voto sea ejercido en secreto y libremente (sin coacciones ni suplantaciones).

b) Debe hacerse mención especial al principio de confidencialidad del voto, pues históricamente ha constituido uno de los escollos más críticos y de vital importancia para la implantación de un sistema de voto electrónico: conseguir que la identidad de los votantes no pueda ser vinculada al voto emitido en ninguna de las fases del proceso de votación. La solución a este punto requiere evitar cualquier registro de traza voto-votante. Éste es uno de los aspectos que permiten certificar la validez del sistema[13].

c) Con el propósito de que las personas confíen en el proceso electoral, es necesario que se acoja a la ley y la constitución electoral vigente en el país, las cuales rigen el funcionamiento de las elecciones, evitando cualquier conflicto. En nuestro caso, la legislación electoral española. Estas leyes son la Ley Orgánica del Régimen Electoral General (LOREG) para las elecciones generales, municipales y europeas, y otras leyes de ámbito autonómico para las elecciones autonómicas. Además, el Consejo de Europa elaboró en 2004 una serie de recomendaciones, las Rec (2004)11, firmadas en Estrasburgo, sobre estándares jurídicos, operativos y técnicos para el voto electrónico.

d) Por otro lado, el sistema debe incorporar aspectos relacionados con auditoría y certificación. Se trata de garantizar la máxima transparencia de la información, la integridad de los votos y total exactitud de los resultados producidos en la votación, haciendo cumplir todos los principios electorales, así como la capacidad de detectar el fraude electoral.

   Algunos de los mecanismos para garantizar la auditabilidad son la generación de logs de auditoría a lo largo del proceso de votación, así como la posibilidad de emitir recibos electrónicos para su posterior verificación, entre otros. Estos mecanismos, junto con toda una serie de medidas específicas de seguridad, facilitarán el proceso de certificación.

e) Adicionalmente, en la línea de ofrecer una máxima transparencia, la compañía de software adjudicada deberá facilitar acceso público a todo el código fuente, permitiendo cualquier tipo de inspección, análisis y comprobación. Una minuciosa revisión del código fuente ayudará a descartar la posibilidad de fraude o manipulación de votos a lo largo del ejercicio electoral. Se requiere, por tanto, liberar el código con una licencia de software libre.

f) Hay que hacer especial incidencia también en el aspecto de seguridad. En este sentido, y para evitar el riesgo de manipulación y robo de votos o datos de carácter personal, es esencial que toda la información enviada esté protegida. Es por ello que se utilizará el sistema de encriptación Advanced Encryption Standard (AES) de 256 bits[14], que actualmente es un estándar de la industria. Se utilizarán también redes virtuales privadas. Se trata de garantizar que toda conexión (servidor local y servicios externos) en todo momento sea realizada por medio seguro.

g) La interacción deberá ser táctil y la interfaz intuitiva y simple de manejar, proporcionando un alto nivel de interactividad y usabilidad. Relacionado con ello, el sistema debe cuidar especialmente la navegación y presentación de las diversas opciones de voto, y de manera excepcional teniendo en cuenta al sector de la población a partir de los 65 años.

h) Internacionalización, pues deberá adaptarse a los diferentes idiomas oficiales del país.

---

[11] Deben estar habilitados para votar todos los ciudadanos que cumplan con un conjunto de condiciones, y exclusivamente ellos.

[12] Los ciudadanos que componen el censo electoral deben poder votar en una sola ocasión (principio de voto único), y todos los votos tienen el mismo valor: un ciudadano, un voto.

[13] Es necesario garantizar una estricta separación, evitando la posibilidad de cruce o vinculación de datos entre votantes y votos bajo ninguna circunstancia.

[14] Estándar global de encriptación que tiene una naturaleza abierta (se puede usar tanto en lo público como en lo privado, para fines comerciales o no) y que es un sistema de clave simétrica (también denominado de clave secreta), lo cual le otorga una mayor seguridad. Lo vemos en aplicaciones de mensajería como WhatsApp, programas como WinZip y una variedad de otras tecnologías que usamos comúnmente.

i) Se requiere una solución flexible, es decir, que sea capaz de adaptarse a diferentes tipos de elecciones (parlamentarias, generales, autonómicas, plebiscitarias, etc.).

j) La protección de datos personales es un derecho fundamental recogido en el artículo 18.4 de la Constitución Española y regulado hoy en día por el RGPD y la Ley orgánica 3/2018 (LOPDGDD[15]), que entraron en vigor en 2018 y 2019 respectivamente. Su misión es preservar la privacidad en el tratamiento de los datos personales, brindando al usuario todos sus derechos a la hora de facilitar sus datos personales.

   En particular, por lo que respecta a los datos biométricos, éstos son recogidos en el artículo 9 del RGPD, en la categoría de datos 'especialmente protegidos'. Establece que este tipo de datos, en especial, deben ser considerados y tratados como datos de carácter sensible, y que es requerido el consentimiento explícito por parte del usuario.

   Por otro lado, para cumplir con el compromiso adquirido en el consentimiento informado sobre el uso de datos biométricos y, en especial, como requisito para garantizar el principio de confidencialidad del voto, una vez contrastados con el usuario, dichos datos pasarán a ser borrados definitivamente del sistema, sin ser incorporados a ninguna base de datos.

k) El uso de la inteligencia artificial en la UE estará regulado por la Ley de Inteligencia Artificial (AI Act), la primera ley integral sobre inteligencia artificial (IA) del mundo.

   Es un reglamento propuesto el 21 de abril de 2021 por la Comisión Europea, cuyo objetivo es introducir un marco normativo y jurídico común para la IA, tratando de ofrecer una regulación clara de sus aplicaciones. El Parlamento Europeo votó su posición en junio de 2023, y se están iniciando negociaciones para finalizar la nueva legislación. Finalmente, la ley deberá ser aprobada, y probablemente habrá que esperar hasta principios de 2025 antes de que entre en vigor oficialmente.

   Como aspectos más destacados, se prohíbe la vigilancia biométrica, el reconocimiento de emociones por IA y los sistemas policiales predictivos. Las IA generativas, como el conocido ChatGPT, tendrán requerimientos adicionales de transparencia.

l) Garantizar el acceso al voto (y también al resto de los trámites incluidos en el sistema) al mayor número posible de usuarios, especialmente a las personas con alguna discapacidad. Se contará con tecnología asistiva y dispositivos periféricos específicos para dar soporte al ejercicio del voto y resto de trámites de forma autónoma (diferentes configuraciones de color y la disponibilidad de líneas braille para discapacitados visuales, son algunos ejemplos). Al menos uno de los terminales disponibles en cada colegio electoral deberá estar provisto de tecnología asistiva. Además, tal y como se ha mencionado, el soporte de inteligencia artificial basado en voz estará disponible en todos los terminales.

m) La norma española UNE 139802:2009 (y sus equivalencias: norma europea EN ISO 9241-171:2008 y norma internacional ISO 9241-171:2008) de 29 de Julio de 2009, elaborada por el comité técnico Sistemas y dispositivos para la tercera edad y la discapacidad, sobre requisitos de accesibilidad del software, proporciona directrices y especificaciones de ergonomía para el diseño de una amplia gama de software. Abarca cuestiones relacionadas con personas con la más amplia gama de capacidades físicas, sensoriales y cognitivas, incluyendo a personas con discapacidades temporales y a las personas mayores. Además, intentan ser complementarias con un diseño usable para una gama más amplia de usuarios.

   Por otra parte, la Unión Europea toma como normas de facto las directrices de accesibilidad que produce el WAI[16] (Web Accessibiliy Initiative, del World Wide Web Consortium - W3C), específicas para aplicaciones web.

Además de las restricciones aquí expuestas, podéis sugerir otras que consideréis indispensables para el buen funcionamiento del sistema. Habrá que idear criterios cuantificables, en caso de que no sean proporcionados en el enunciado.

---

[15] Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

[16] https://www.w3.org/WAI/about/