Cada ve que usamos el navegador y buscamos o abrimos una página web lo que estamos haciendo es conectar nuestro ordenador al ordenador, el servidor, en el que vive esa página o sitio web. El tiempo que transcurre desde que nos conectamos a ese servidor hasta que saltamos a otra página web o dejamos el ordenador para hacer otra cosa se llama “sesión”.

Cuando iniciamos una sesión, el servidor en donde está el sitio web envía un pequeño archivo a tu navegador en el que está tu número de identificación, de manera que si después de haber ido a otros sitios web o haber vuelto al ordenador, te vuelves a conectar a ese sitio, el servidor sabrá que es tu ordenador el que se está conectando. Es decir, este pequeño archivo le sirve al servidor para identificarte y recordarte. Ese archivo que utilizan todos los servidores cada vez que usamos el navegador es lo que llamamos “cookies” e identifica tu ordenador y lo recuerda a pesar de que no has tenido que darte de alta ni escribir tu nombre de usuario y tu contraseña.

Hay varios tipos de cookies:

Las de *sesión*, que sirven para que funcione el botón de “atrás” de tu navegador y que se elimina cuando finalizas la sesión.

Las *persistentes*, que se quedan en tu ordenador hasta que tú mismo las borres yendo a las Preferencias, y en la parte de Privacidad puedes seleccionar cuáles aceptar o no, o a la Historia de tu navegador y borres todo lo que hay allí.

Estos dos tipos se suelen conocer como cookies de origen por que proceden de los sitios a los que has navegado de manera voluntaria. Sin embargo, muchos de estos sitios a los que navegas de manera voluntaria venden espacio en su sitio web para que otros publiquen sus anuncios. Pues bien, estos anuncios suelen llevar sus propias cookies, las cookies de *terceros* y, sin que lo sepas, las empresas que publican esos anuncios las utilizan para rastrearte y saber lo que has hecho, en esa sesión y, a veces, cuando vas a otros sitios web sin haber borrado antes las cookies. Algunos navegadores han comenzado a eliminarlas y lo cierto es que tu experiencia no cambiará mucho si se eliminan porque, desgraciadamente, dejamos rastros de quiénes somos y qué hacemos de muchas otras formas.

¿Por qué hacen esto los servidores? Hay dos razones fundamentales: eficacia y rastreo.

La eficacia tiene que ver con la oferta de un servicio más personalizado y más rápido, es decir, que al enviarte las cookies a tu navegador cuando vuelves a conectarte a ese sitio web el servidor sabe que eres tú y te ofrecerá la información en la que parece que estás interesado, por ejemplo, música o deportes. También se usan para que tu carrito de la compra se pueda recuperar incluso si cierras el navegador por error o refrescas la página por alguna razón. La eficacia está vinculada a la personalización, pero eso quiere decir que esta personalización (que incluye identificación y recuerdo) se puede comer poco a poco tu privacidad, porque los servidores a los que te conectas “saben” lo que te interesa y lo que haces cuando navegas por Internet.

Esta personalización está relacionada con las tres monedas digitales (datos, dinero y atención). La personalización le sirve al sitio web al que te conectas para eso, “personalizar” los anuncios que aparecen en ese mismo sitio web, de manera que de la navegación que has hecho deducen un poco de quién eres qué te puede gustar y qué podrías comprar si los anuncios adecuados atraen tu atención. Esos espacios para los anuncios están a la venta (en realidad se subastan de manera automática en un sistema que funciona de manera instantánea y que los compradores de espacios para anuncios) y las empresas que quieren venderte zapatos o camisas o entradas para un concierto, compran esos espacios en función de quién eres, la hora del día que es, dónde estás y tus comportamientos anteriores, entre otras cosas.

Entonces, la personalización tiene un segundo componente que es el rastreo de tu identidad y de tu comportamiento. Imagínate que permitiéramos que alguien nos siguiera todo el día por la calle y apuntara en una libreta cada cosa que hacemos para luego vender esa información a sus clientes, que te llamarían a casa o te pararían por la calle para ofrecerte sus productos.

Este rastreo usa todas las pistas que hemos dejado en la interacción digital (recuerda, todo lo que hacemos en una pantalla se guarda y se analiza) para luego vender esa información. No solo la tuya, sino la de todos los que van a esos servidores, porque a mayor volumen de datos de más gente más fácil es predecir qué vamos a hacer y quiénes somos.

Como hemos visto, la experiencia de navegación puede ser igual de buena si no hay cookies de *terceros.* Con el objetivo de proteger la privacidad de los ciudadanos, la Unión Europea y países como España han desarrollado leyes que obligan a todos los servicios de Internet a preguntar cada vez que comienzas una sesión si quieres solamente las cookies esenciales o aceptas todas, incluso las de terceros. Debes saber que no hay ningún problema si solo aceptas las esenciales, que son las necesarias para que ese sitio web funcione de manera adecuada.

Pero, ¿qué ocurre con los sitios web que piden que te registres con un nombre de usuario y de una contraseña que luego tienes que reutilizar cada vez que comienzas una sesión nueva? En ese caso, se siguen cumpliendo los principios que regulan el funcionamiento de las cookies y las razones por las que el sitio web las usa, pero además ahora tienen ese mecanismo de identificación reforzada que es el registro. Ya saben quién eres y por eso puedes entrar a “tu” página de Instagram, Google Classroom, TikTok, o Youtube. Es decir, que estas plataformas que no te dejan que las uses a menos que te identifiques van creando una imagen de cada uno de los usuarios que se compone de los datos y la atención que dejamos cada vez que les decimos “¡Hey!, aquí estoy, y quiero entrar a mi sitio dentro de tu plataforma para jugar con mis amigos o ver sus últimos “posts” o compartir una foto con ellos!”

¿Y los teléfonos móviles? En los teléfonos móviles podemos usar los navegadores de la misma forma que lo hacemos en un ordenador y, en este caso, las cookies funcionan de la misma forma. Pero, además, el móvil tiene mecanismos súper reforzados de personalización y rastreo porque para que el móvil funcione lo tienes que dar de alta a través de Android (Google) o Apple, de manera que estas plataformas saben lo que estás haciendo siempre que lo tienes encendido y, a veces, incluso cuando está apagado. Lo mismo ocurre con las apps del teléfono (o de la consola de juegos o las gafas de realidad virtual) porque, como te habrás dado cuenta, no puedes usarlas (sí te las puedes bajar) sin haber pasado por el Mercado de Android (Google) o la Tienda de Apple, para lo que necesitas que tu teléfono esté registrado. Una vez has bajado la app a tu teléfono, tienes que darte de alta en la app, y dejar así las señales que permitirán la personalización de la experiencia y a la vez que tu experiencia se pueda vender gracias al rastreo de los datos que has ido dejando en cada paso de la interacción con las pantallas.

Lo importante es saber que datos, dinero y atención funcionan de manera coordinada en el Internet de las plataformas. También que estos tres elementos afectan a nuestra vida privada y a nuestro comportamiento y que una educación apropiada y una acción de nuestros gobiernos son las dos herramientas más poderosas que tenemos para conservar la privacidad y la autonomía de nuestros hijos en este mundo digital en el que estamos inmersos.