En los últimos años, los servicios de redes sociales, como Facebook o LinkedIn, han experimentado un crecimiento exponencial. Los usuarios valoran positivamente sus muchas funcionalidades tales como compartir fotos, o búsqueda de amigos y trabajo. En general, los usuarios aprecian los beneficios que las redes sociales les aportan. Sin embargo, mientras el uso de redes sociales se ha convertido en rutina para mucha gente, brechas de privacidad que pueden ocurrir en redes sociales han aumentado los recelos de los usuarios. Por ejemplo, es sencillo encontrar en las noticias casos sobre personas que han perdido su empleo debido a algo que compartieron en una red social. Para facilitar la definición de los ajustes de privacidad, los proveedores de servicios emplean controles de acceso sencillos que normalmente se basan, de forma exclusiva, en listas o círculos de amigos. Aunque estos controles de acceso son fáciles de configurar por un usuario medio, investigaciones recientes indican que éstos carecen de elementos tales como la intensidad de los vínculos personales, que juegan un papel clave en cómo los usuarios deciden qué compartir y con quién. Además, a pesar de la simplicidad de los controles de acceso, investigaciones sobre privacidad en redes sociales señalan que los usuarios han de esforzarse para controlar de forma efectiva como su información fluye en estos servicios.

Para ofrecer a los usuarios un marco de privacidad más robusto, investigaciones recientes proponen un nuevo paradigma para controles de acceso basado en relaciones. A diferencia de los controles de acceso tradicionales donde los permisos se otorgan en base a usuarios y sus roles, este paradigma emplea elementos sociales como la relación entre el propietario de la información y su audiencia potencial (por ejemplo, sólo mis hermanos pueden ver la foto). Los controles de acceso que siguen este paradigma ofrecen a los usuarios mecanismos para el control de la privacidad que representan de una forma más natural como los humanos razonan sobre cuestiones de privacidad. Además, estos controles de acceso pueden lidiar con problemáticas específicas que presentan las redes sociales. Específicamente, los usuarios comparten de forma habitual información que atañe a muchas personas, especialmente a otros miembros de la red social. En tales situaciones, dos o más personas pueden tener preferencias de privacidad que entran en conflicto. Cuando esto ocurre, no hay una configuración correcta de privacidad que sea evidente. Estas situaciones son normalmente identificadas como escenarios de privacidad multiusuario.

Dado que los controles de acceso basados en relaciones son complejos para el usuario promedio de redes sociales, los proveedores de servicios no los han adoptado. Por lo tanto, para permitir la implementación de tales controles de acceso en redes sociales actuales, es necesario que se ofrezcan herramientas y mecanismos que faciliten su uso. En este sentido, esta tesis presenta cinco contribuciones: (1) una revisión del estado del arte en manejo de privacidad en redes sociales que permite identificar los retos más importantes en el campo, (2) una herramienta para obtener automáticamente la intensidad de los vínculos personales y las comunidades de usuarios, (3) un nuevo control de acceso que emplea comunidades, identificadores individuales, la intensidad de los vínculos personales, y etiquetas de contenido, (4) un modelo novedoso para representar y razonar sobre escenarios de privacidad multiusuario que emplea tres tipos de características: factores contextuales, preferencias de usuario, y argumentos de usuario; y, (5) Muppet, una herramienta que recomienda configuraciones de privacidad en escenarios de privacidad multiusuario.

Las contribuciones de esta tesis emplean técnicas de inteligencia artificial tales como aprendizaje automático, minería de datos, y colaboración distribuida. Las contribuciones han sido validadas por medio de estudios con participantes humanos. Concretamente, tres estudios con 38, 50, y 988 participantes han aportado los datos que han sido empleados para evaluar cada contribución. Los resultados muestran que los controles de acceso para redes sociales pueden ser mejorados mediante herramientas que automatizan tareas relacionadas con privacidad (BFF y Muppet) y modelos formales que representan fidedignamente como los humanos razonan sobre la privacidad.