UNIVERSIDAD DE SAN MARTIN DE PORRES FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

RESUMEN SEMANA 14

INTEGRANTES:

BARRANTES CONTO, FABRICIO GABRIEL

PROFESOR:

RUEDA ÑOPO, NORMA ADRIANA

LA MOLINA, PERÚ

2025– I

Resumen del grupo N°9

En la exposición se aborda de manera profunda y crítica la problemática de la vigilancia masiva en la era digital, destacando tanto los beneficios potenciales como los riesgos asociados a estas prácticas. Se analiza cómo los avances tecnológicos, como la inteligencia artificial, el reconocimiento facial, los algoritmos predictivos, las cámaras inteligentes y la geolocalización, han proporcionado a los gobiernos y empresas herramientas poderosas para recopilar, procesar y analizar grandes volúmenes de datos personales. Aunque estas tecnologías pueden ser utilizadas para fines legítimos, como la protección de la seguridad nacional, la prevención del crimen o la mejora de servicios públicos, también generan preocupaciones serias en torno a los derechos humanos y las libertades fundamentales.

Uno de los aspectos centrales del análisis es la tensión ética generada por la vigilancia masiva: cómo garantizar la protección de la seguridad sin sacrificar la privacidad y las libertades individuales. Se menciona el caso Snowden 2013, que reveló la magnitud de la vigilancia estatal y expuso cómo las prácticas de recopilación de datos, muchas veces sin conocimiento ni consentimiento de los individuos, amenazan el derecho a la privacidad y la libertad de expresión. La existencia de controles insuficientes y la falta de regulación específica en tecnologías emergentes contribuyen a la creación de vacíos legales que pueden ser explotados para justificar acciones invasivas y, en algunos casos, discriminatorias.

El ensayo también señala que la vigilancia masiva puede generar un “efecto panóptico” una sensación de vigilancia constante que puede afectar la conducta de los ciudadanos, promoviendo comportamientos de autocensura y limitando la libertad individual. Cuando las personas sienten que sus movimientos y decisiones están siendo observados en todo momento, se produce un impacto psicológico que puede socavar los valores democráticos y la confianza en las instituciones. Además, la afirmación de que la vigilancia masiva puede convertirse en una herramienta de control social refuerza la preocupación por el riesgo de que estas prácticas se utilicen para limitar la libertad y reforzar un Estado de vigilancia autoritario.

Otra problemática importante que se destaca es el impacto diferencial de la vigilancia en distintos grupos sociales. Las tecnologías, en ocasiones, reproducen sesgos sociales y raciales existentes, afectando desproporcionadamente a comunidades minoritarias o vulnerables. La falta de marcos regulatorios adecuados, combinada con sesgos en los algoritmos y prácticas opacas, puede resultar en discriminación y exclusión social. La necesidad de normativas específicas para tecnologías como el reconocimiento facial, que respalden la protección de los derechos de estos grupos, resulta fundamental para evitar estos efectos adversos.

El texto también hace énfasis en los vacíos legales y en la insuficiencia de la regulación existente, que muchas veces no avanza en paralelo al desarrollo tecnológico. La rapidez con la que surgen nuevas herramientas no siempre se acompaña de una legislación clara, generando un escenario donde la incertidumbre jurídica favorece el uso abusivo y sin control de los datos. La falta de transparencia en la gestión de la información, así como la existencia

de intereses comerciales, convierten a la vigilancia en una práctica potencialmente peligrosa para la democracia y los derechos humanos.

No obstante, también se reconocen ciertos argumentos a favor de la vigilancia masiva, como su papel en la detección de amenazas y delitos, permitiendo a las autoridades actuar preventivamente y reducir riesgos potenciales. Se sostiene que, si bien la vigilancia puede ser una herramienta útil para la protección ciudadana, su eficacia y legitimidad dependen en gran medida de la existencia de controles adecuados, transparencia en los procesos y mecanismos de rendición de cuentas. La implementación de marcos éticos y normativos sólidos, así como la participación ciudadana en la deliberación sobre estas prácticas, son elementos esenciales para equilibrar la seguridad y la protección de los derechos.

Finalmente, el ensayo aboga por la necesidad de promover una cultura de responsabilidad digital, donde tanto los responsables del diseño y uso de las tecnologías como los usuarios sean conscientes de las implicaciones éticas, sociales y legales. Es indispensable fortalecer las instituciones democráticas, fomentar la educación en derechos digitales y promover políticas públicas que aseguren la protección de la privacidad y los derechos fundamentales en un contexto cada vez más marcado por la tecnología.