UNIVERSIDAD CATÓLICA BOLIVIANA “SAN PABLO”

UNIDAD ACADÉMICA LA PAZ

MATERIA: Introducción a los Negocios Internacionales

“LIBRO DE APUNTES”

PRESENTADO POR:

- Nicolas Juan Garcia Suxo
-Bruno Alfonso Gumiel Zeballos
- Rous Quenallata Mamani
- Pamela Marlene Quispe Clemente
- Nick Kevin Ticona Condori

PROFESOR:
Gonzalo Chavez Alvarez

LA PAZ- BOLIVIA
2025

5. La Transformación Digital y sus Efectos sobre las Relaciones Internacionales

Autores base:

- Harari, Y. N. (2018). *21 Lecciones para el Siglo XXI*. Capítulos 4 y 5.
- Segura, A. (2019). *La era de la disrupción digital*. Capítulos 1 y 2.
- Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities*. Working Paper.
- Singer, P. W. y Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Capítulo 1.

5.1 El Cambio Tecnológico y sus Oportunidades y Riesgos para la Democracia, la Privacidad y la Soberanía

Fundamentos de Harari: Tecnología y Sociedad

Harari, en *21 Lecciones para el Siglo XXI*, discute cómo las tecnologías emergentes, como la **inteligencia artificial** (IA) y el **big data**, están alterando las estructuras sociales, políticas y económicas.
Capítulo 4 y 5 se centran en:

- **Impacto de la IA y los algoritmos** en la toma de decisiones, donde los gobiernos, corporaciones y otras entidades se basan en datos masivos para influir en comportamientos, elecciones y mercados.
- **La privacidad y la soberanía** se ven amenazadas por la recopilación masiva de datos. El **Estado** pierde control sobre la información que antes era parte de su soberanía.

Riesgos para la Democracia y la Privacidad

- Los **gobiernos autoritarios** pueden usar tecnologías de vigilancia masiva para **controlar a sus ciudadanos**, como se ve en **China** con el uso del **sistema de crédito social**.
- La **privacidad** está en constante amenaza con el **control de datos personales**, que pueden ser utilizados para manipular elecciones o **vulnerar la autonomía individual**.
- **Censura digital** y **manipulación de redes sociales** son herramientas utilizadas para influir en procesos democráticos, como se vio en **la interferencia rusa en las elecciones de EE.UU. 2016**.

Relación con Bolivia

En Bolivia, el cambio tecnológico presenta tanto **oportunidades** como **desafíos**:

- **Oportunidades**: La digitalización de la economía boliviana puede permitir mejorar sectores como la minería (e.g., litio), comercio electrónico, y la infraestructura energética.

- **Riesgos**: La **vulnerabilidad en ciberseguridad** podría permitir a actores externos influir en la política interna, además de la **violación de privacidad** debido a la falta de regulación digital en el país.

5.2 La Revolución Digital y sus Implicaciones Geopolíticas y Económicas

Fundamentos de Segura: Disrupción Digital

En *La Era de la Disrupción Digital*, Segura analiza cómo la **transformación digital** está afectando la **competencia global**.

En los **Capítulos 1 y 2**, Segura argumenta que la revolución digital no solo está alterando los modelos de negocio, sino también **reconfigurando las relaciones internacionales**, ya que:

- **El poder económico ahora está en manos de los datos y la conectividad**.
- El **cambio geopolítico** se basa en **quién controla las infraestructuras tecnológicas** (5G, IA, satélites, etc.).
- **Las economías emergentes** como **China** y **India** están adoptando tecnologías más rápidamente que las economías tradicionales (EE.UU. y Europa).

Implicaciones Económicas y Geopolíticas

- La **digitalización de las economías** provoca una **competencia** por **acceso a datos**, **tecnologías emergentes** y **control de plataformas digitales** (e.g., Google, Facebook, Alibaba, Tencent).
- **Riesgos geopolíticos**: Los países que no se adaptan a la nueva economía digital **quedan marginados** y su soberanía se ve comprometida por **dependencia tecnológica**.

Relación con Bolivia

- Bolivia debe **adaptarse** a la digitalización para mejorar su **competitividad económica** y evitar quedar atrás.
- **China**, con sus empresas como **Huawei**, está proporcionando infraestructura digital en Bolivia, pero esto también **crea dependencia tecnológica** y pone en duda la **soberanía digital** de Bolivia frente a potencias extranjeras.

Ejemplo actual:

La adopción de tecnologías en el sector **financiero** (como el uso de plataformas de pago móvil) es una oportunidad, pero también presenta riesgos de **vulnerabilidad cibernética**.

5.3 La Ciberseguridad y la Ciberguerra como Amenazas y Desafíos Transnacionales

Fundamentos de Nye: Gobernanza Cibernética Global

En su trabajo *The Regime Complex for Managing Global Cyber Activities* (2014), Nye examina cómo la **ciberseguridad** se ha convertido en un desafío **transnacional** debido a:

- **La falta de reglas claras**: Los regímenes internacionales para gestionar **ciberseguridad** y **actividades cibernéticas** son fragmentados.
- **La ciberguerra**: Los Estados utilizan **ataques cibernéticos** como herramienta estratégica para **desestabilizar** a otros países, sin recurrir a la guerra tradicional.
- **El complejo régimen**: La gobernanza global de internet está fragmentada entre actores estatales y no estatales (gobiernos, empresas tecnológicas, ONGs, etc.).

Desafíos en la Gobernanza Global de Internet

- **Cibercrimen**: A medida que los ciberataques se vuelven más sofisticados, los países enfrentan desafíos para proteger su infraestructura.
- **Ciberguerra**: La competencia en el ciberespacio puede tener consecuencias tan graves como un conflicto militar.
- **Regulaciones internacionales**: No existe un marco global único que regule internet y ciberseguridad.

Relación con Bolivia

- Bolivia enfrenta desafíos de **ciberseguridad**:
    - Las **infraestructuras digitales** son vulnerables a ciberataques de actores externos (como **hackers** y **agentes estatales**).
    - La **gobernanza digital** en Bolivia no está lo suficientemente madura para prevenir manipulaciones externas.

Ejemplo actual:
El **hackeo de instituciones financieras** o la **interferencia en elecciones** usando plataformas digitales (similar a lo sucedido en otras democracias) representa un riesgo real para Bolivia.

5.4 Ciberseguridad y Ciberguerra como Desafíos Transnacionales

Fundamentos de Singer y Friedman: La Amenaza Cibernética

En *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), Singer y Friedman explican que:

- La **ciberseguridad** es un desafío global porque los actores **no estatales** (hackers, grupos terroristas) y los **estados** (EE.UU., China, Rusia) operan sin reglas claras.
- La **ciberguerra**: los ataques cibernéticos pueden **dañar infraestructuras críticas** como energía, sistemas financieros y redes de comunicación.

Implicaciones para la seguridad global

- **La ciberguerra** puede **desestabilizar economías** y **sociedades** sin disparar un solo tiro.
  Países pequeños como Bolivia enfrentan dificultades para protegerse de ataques debido a la falta de **capacidades tecnológicas**.

Relación con Bolivia

- Bolivia debe **invertir en ciberseguridad** para evitar ataques que puedan **desestabilizar su infraestructura**.
  Ejemplo: **el sector energético y financiero** son vulnerables.
- Bolivia debe formar alianzas estratégicas con **actores internacionales** que puedan proporcionar **tecnología de protección**.

Conclusiones Generales

La **transformación digital** es un fenómeno que tiene **profundas implicaciones** para las relaciones internacionales:

- **Oportunidades**: Mejora de competitividad, inclusión financiera, acceso a mercados internacionales.
- **Riesgos**: Pérdida de privacidad, amenazas a la democracia, ciberataques.
- **Gobernanza digital**: Necesidad urgente de **cooperación internacional** para establecer reglas claras en cuanto a **privacidad**, **ciberseguridad** y **ciberguerra**.

Bolivia debe abordar estos retos de manera estratégica, no solo para **protegerse** de amenazas, sino también para **aprovechar las oportunidades** que ofrece la transformación digital.