TUDO BEM?... *TUDO LEGAL?*

Analizando la investigación en **fuentes abiertas**

Miguel Sumer Elías

sumerelias

Abogado especializado en
Cibercrimen, **Privacidad** y **Negocios Digitales**.

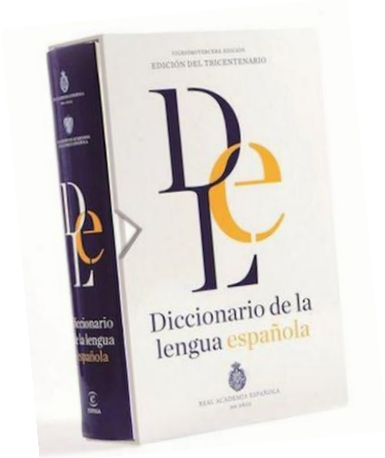
Profesor de **Derecho Informático** en
diversas instituciones latinoamericanas.

Director de:

www.informaticalegal.com

www.internetresponsable.com

¿Qué es hacer “inteligencia”?



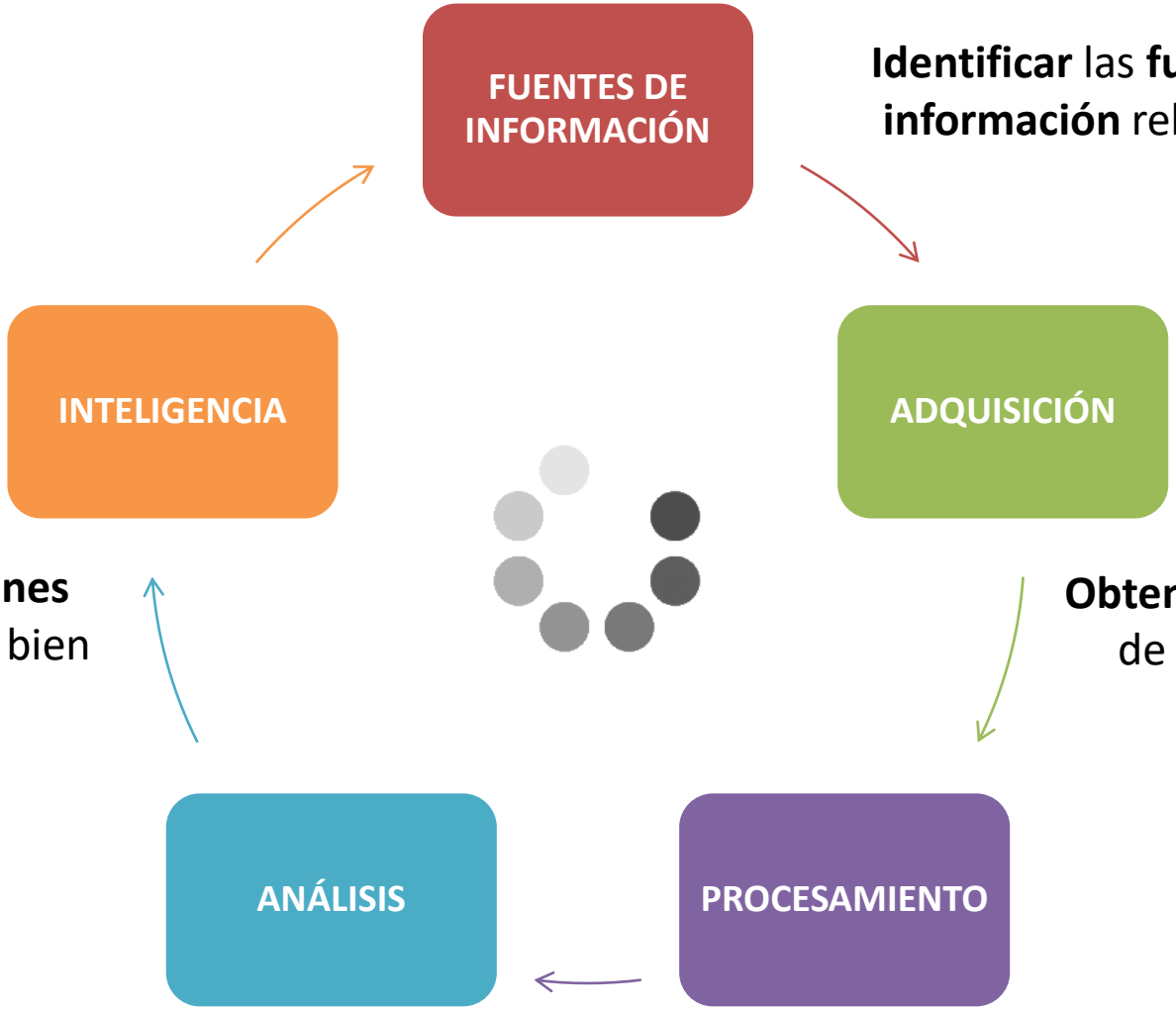
Inteligencia

1. Capacidad de **entender** o **comprender**.
2. Capacidad de **resolver problemas**.
3. **Conocimiento**, **comprensión**, **acto de entender**.
4. Sentido en que se puede tomar una proposición, un dicho o una expresión.
5. Habilidad, destreza y experiencia.
6. Trato y correspondencia secreta de dos o más personas o naciones entre sí.
7. Sustancia puramente espiritual.
8. **Servicio de inteligencia**.

Servicio de Inteligencia

1. Organización del Estado que proporciona al Poder Ejecutivo **análisis** e **información** para mejorar la **toma de decisiones** estratégicas orientadas a prevenir o neutralizar amenazas y a defender los intereses nacionales.

Inteligencia. Distintas etapas



Identificar las **fuentes de información** relevantes.

Obtener la **información** de dichas fuentes.

Procesar la información encontrada.

Analizar la información y encontrar **patrones**.

Sacar **conclusiones** con información bien presentada.

Fuentes abiertas y cerradas

¿**Qué es lo que determina** si una fuente es **abierta** o **cerrada**?

Depende si el **propietario de la información** estableció o no **medidas de autenticación y seguridad** para **impedir** el **acceso no autorizado**.

Repasando el concepto de “OSINT”

Es el **conocimiento** y **explotación de** **<u>fuentes de acceso público</u>** para **realizar inteligencia** y **tomar decisiones**.

La delgada línea entre lo permitido y lo prohibido

Reflexionemos sobre el límite de lo tolerado…

Lo tolerado está prohibido…
pero se tolera…

Expectativa vs. Realidad

Realidad

Un **investigador** puede utilizar herramientas de OSINT para acceder a una **fuente abierta** y obtener información.

Expectativa de Seguridad del usuario

Expectativa de Privacidad del usuario

¿Y si un **usuario** cree que sus datos están en una **fuente cerrada** cuando en realidad no lo es?

¿Cuál es el **límite** para que esa **obtención sea legítima**?

¿Esa **expectativa o desconocimiento** es **suficiente argumento** para **desestimar la prueba**?

Reflexión. OSINT vs. Privacidad

¡DEPENDE!

¿Puedo **utilizar cualquier** información que encuentro en **"fuentes públicas"**?

¿La información es **pública** por el solo hecho de **estar en la web?**

¿Toda **información pública** es **publicable** y cuenta con la autorización del propietario**?**

Algunos tips…

- Recolectar la prueba de acuerdo al **debido proceso** con la **legalidad y las autorizaciones** correspondientes.

- Respetar **las leyes de privacidad y de protección de datos personales**.

- Cumplir con la **ley del país en el cual se vaya a investigar**. Lo que en un país es público, en otro por ahí no.

Investigaciones criminales con OSINT

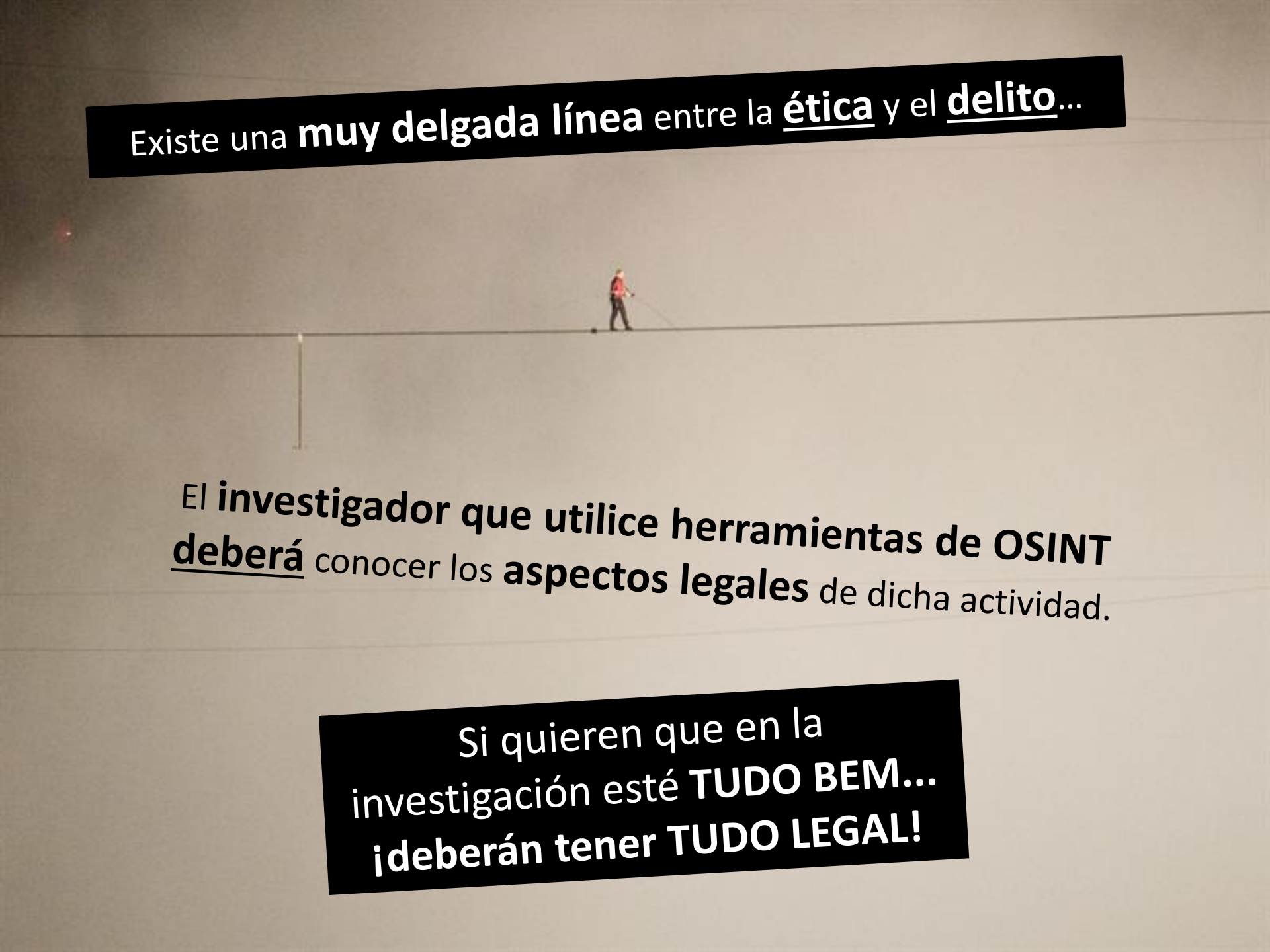
¿Son **herramientas lícitas** o **ilícitas**?

¿Las empresas **autorizan** estas prácticas?

Analicemos algunas acciones **realizadas sin autorización**...

Obtener información bancaria manipulando psicológicamente a los usuarios.	**Ingeniería social**	**Estafa**
Probar la vulnerabilidad de un sistema o dato informático.	**Pen-Test | Hacking**	**Acceso ilegítimo a datos**
Demostrar en vivo las vulnerabilidades reales encontradas en sistemas ajenos.	**Demo**	**Violación de la privacidad** **Apología del delito**
Explotar esas vulnerabilidades, alterando o inutilizando sitios, datos o sistemas.	**Cracking** **Ingeniería inversa**	**Daño o sabotaje informático** **Interrupción de comunicaciones**
Desarrollar programas que puedan detectar y explotar esas vulnerabilidades.	**Arte | Malware** **Exploit 0-Day**	**Distribución de programas destinados a causar daños**
Analizar una nueva "tendencia tecnológica" que busque errores del fabricante para hacerlo responsable de los mismos.	**Prueba de Concepto (PoC)**	**Espionaje | Acceso ilegítimo**

Existe una **muy delgada línea** entre la **ética** y el **delito**…



El **investigador que utilice herramientas de OSINT deberá** conocer los **aspectos legales** de dicha actividad.

Si quieren que en la investigación esté **TUDO BEM… ¡deberán tener TUDO LEGAL!**

Miguel Sumer Elías
www.informaticalegal.com
miguel@informaticalegal.com
@sumerelias

MUCHAS GRACIAS