Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Tipificación de los Delitos en Argentina

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

La **tipificación de los delitos** constituye uno de los pilares fundamentales del Derecho Penal y adquiere especial relevancia en el ámbito de las Tecnologías de la Información (TI), donde las conductas ilícitas evolucionan con rapidez y requieren una adecuada encuadración jurídica. Tipificar un delito implica describir en la ley una conducta específica y establecer una sanción correspondiente. Para que una acción sea considerada delito, debe reunir determinados elementos estructurales: ser una **conducta**, **típica**, **antijurídica** y **culpable**.

En el contexto de los sistemas de información, la tipificación resulta clave para encuadrar jurídicamente hechos como el acceso indebido a bases de datos, el fraude electrónico, el ransomware o la interceptación ilegal de comunicaciones. Sin una adecuada tipificación, las organizaciones y el Estado enfrentan dificultades para sancionar conductas que afectan activos digitales estratégicos.

Para estudiantes de licenciatura en administración, comprender la estructura jurídica del delito permite integrar la dimensión legal dentro de la gestión tecnológica, evaluar riesgos regulatorios y diseñar políticas de cumplimiento normativo alineadas con la legislación vigente.

Desarrollo

1. Elementos Estructurales del Delito

En la teoría del delito, un hecho es penalmente relevante cuando reúne cuatro elementos esenciales:

1. Conducta.
2. Tipicidad.
3. Antijuridicidad.
4. Culpabilidad.

Estos elementos se aplican tanto a delitos tradicionales como a delitos informáticos.

---

2. La Conducta

La **conducta** es el comportamiento humano voluntario que puede consistir en una acción (hacer algo) o en una omisión (no hacer algo cuando se tenía el deber jurídico de hacerlo).

En el ámbito de TI:

- Acción: ingresar sin autorización a un sistema.
- Omisión: no implementar medidas de seguridad obligatorias cuando existe deber legal de protección de datos.

Sin conducta humana voluntaria no existe delito.

---

3. La Tipicidad

La **tipicidad** implica que la conducta realizada debe coincidir exactamente con la descripción contenida en la ley penal (tipo penal).

Ejemplo en TI:

Si la ley penal describe como delito “acceder indebidamente a un sistema informático protegido”, solo será delito la conducta que se ajuste a esa descripción.

La tipicidad garantiza el principio de legalidad: no hay delito sin ley previa que lo establezca.

En el entorno digital, la tipificación resulta compleja debido a la evolución tecnológica constante.

---

4. La Antijuridicidad

La **antijuridicidad** significa que la conducta típica debe ser contraria al ordenamiento jurídico y no estar justificada.

Existen causas de justificación, como:

- Legítima defensa.
- Cumplimiento de un deber.
- Ejercicio legítimo de un derecho.

En el ámbito tecnológico:

Un perito informático autorizado judicialmente a ingresar en un sistema no comete delito, aunque la conducta coincida materialmente con el tipo penal de acceso indebido, porque existe una causa de justificación.

---

5. La Culpabilidad

La **culpabilidad** implica que el autor debe ser reprochable por su conducta. Esto supone:

- Capacidad de comprender la ilicitud.
- Posibilidad de actuar de otra manera.

Dentro de la culpabilidad se distinguen dos formas principales de imputación subjetiva:

1. Dolo.
2. Culpa.

---

6. Dolo y Culpa

6.1 Dolo

El **dolo** implica intención y conocimiento. El autor sabe lo que hace y quiere realizar la conducta prohibida.

Ejemplo en TI:

Un empleado que deliberadamente roba información confidencial para venderla a la competencia actúa con dolo.

El dolo puede ser:

- Directo (quiere el resultado).
- Eventual (acepta la posibilidad del resultado).

6.2 Culpa

La **culpa** implica negligencia, imprudencia o impericia. El autor no desea el resultado ilícito, pero actúa sin la diligencia debida.

Ejemplo:

Un administrador de sistemas que no actualiza parches críticos y permite una brecha de seguridad puede incurrir en responsabilidad culposa.

La diferencia esencial:

- En el dolo hay intención.
- En la culpa hay falta de cuidado.

Desde la perspectiva administrativa, esta distinción es fundamental para evaluar responsabilidades internas.

---

7. Aplicación en Delitos Informáticos

En delitos informáticos, la tipificación puede incluir:

- Acceso ilegítimo a sistemas.
- Interceptación indebida.
- Manipulación de datos.
- Fraude electrónico.
- Distribución de malware.

Cada conducta debe analizarse bajo los cuatro elementos estructurales del delito.

---

8. Derecho Codificado vs. Sistemas No Codificados

La forma en que se tipifican los delitos depende del sistema jurídico.

8.1 Sistemas de Derecho Codificado (Civil Law)

En los sistemas de derecho codificado, como los de tradición continental europea y latinoamericana, los delitos se encuentran descritos en códigos penales escritos.

Características:

- Normas detalladas.
- Tipos penales específicos.
- Interpretación basada en texto legal.

La tipificación es estricta y el juez no puede crear delitos por analogía.

8.2 Sistemas de Common Law

En jurisdicciones de tradición anglosajona, como Estados Unidos o Reino Unido, el sistema se basa en precedentes judiciales.

Características:

- Mayor flexibilidad.
- Importancia de la jurisprudencia.
- Evolución interpretativa.

En materia de delitos informáticos, esta diferencia puede influir en la rapidez de adaptación normativa.

---

9. Impacto para la Administración y TI

Para organizaciones que operan internacionalmente, comprender diferencias jurisdiccionales es esencial.

Ejemplo:

- Una conducta puede estar tipificada como delito en una jurisdicción y no en otra.
- Las obligaciones de protección de datos varían según el sistema jurídico.

La gestión de cumplimiento (Compliance) debe considerar:

- Marco legal local.
- Responsabilidad penal corporativa.
- Obligaciones regulatorias.

---

10. Dimensión Estratégica

Desde la perspectiva administrativa, la tipificación penal:

- Define riesgos legales.
- Establece límites operativos.
- Orienta políticas internas.
- Influye en decisiones tecnológicas.

La prevención de delitos informáticos requiere integrar seguridad tecnológica y asesoramiento jurídico.

---

11. Ejemplo Integrado

Supongamos que un empleado descarga bases de datos sin autorización.

Análisis:

- Conducta: descarga voluntaria.
- Tipicidad: encuadre en acceso indebido o revelación de secretos.
- Antijuridicidad: no existe autorización.
- Culpabilidad: si actúa intencionalmente, hay dolo.

El análisis jurídico permite determinar responsabilidad.

Conclusión

La tipificación de los delitos constituye el mecanismo jurídico que permite transformar conductas humanas en infracciones penalmente sancionables. En el ámbito de las Tecnologías de la Información, donde las acciones digitales pueden generar daños significativos, resulta esencial comprender que todo delito requiere conducta, tipicidad, antijuridicidad y culpabilidad.

La distinción entre dolo y culpa permite diferenciar entre intención y negligencia, aspecto crucial para evaluar responsabilidades en entornos tecnológicos complejos. Asimismo, la diferencia entre sistemas de derecho codificado y sistemas basados en precedentes judiciales influye en la forma en que se regulan y sancionan los delitos informáticos.

Para los futuros administradores, integrar la dimensión jurídica en la gestión tecnológica es indispensable para reducir riesgos regulatorios, fortalecer el cumplimiento normativo y garantizar la sostenibilidad organizacional en un entorno digital globalizado.

Preguntas de autoevaluación

1. ¿Cuáles son los cuatro elementos estructurales del delito?
2. ¿Qué diferencia existe entre dolo y culpa en el ámbito de delitos informáticos?
3. ¿Por qué la tipicidad garantiza el principio de legalidad?
4. ¿Cómo influyen las diferencias entre derecho codificado y common law en la regulación tecnológica?
5. ¿Por qué la comprensión de la tipificación penal es relevante para la gestión de riesgos en TI?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.