

ПОЛИТИКИ И ПРАКТИКИ ИНТЕРНЕТ- ИНДУСТРИИ ДЛЯ ХРАНЕНИЯ ДАННЫХ И ОБЕСПЕЧЕНИЯ ДОСТУПА ПРАВООХРАНИТЕЛЬНЫМ ОРГАНАМ



**Национальный Центр по защите
Персональных Данных**

**Серджиу Бозиану
Управление учета и контроля**

План презентации:

I) Правовая основа

- (a) Обязательство по хранению данных
- (b) Пути доступа компетентных органов

II) Практика разных компаний

- (a) Обязательство по хранению данных
- (b) Предоставление доступа компетентным органам

III) Защита данных в контексте сохранения

- (a) Юридические гарантии
- (b) Контекст ЕС и последствие для Республики Молдова

I) Правовая основа

--- Генеральный обзор ---

**ЗАКОН № 20 от
03.02.2009**

о предупреждении и
борьбе с преступностью в
сфере компьютерной
информации

**ЗАКОН № 241 от
15.11.2007**

об электронных
коммуникациях

ЗАКОН № 59 от 29.03.2012

о специальной розыскной
деятельности

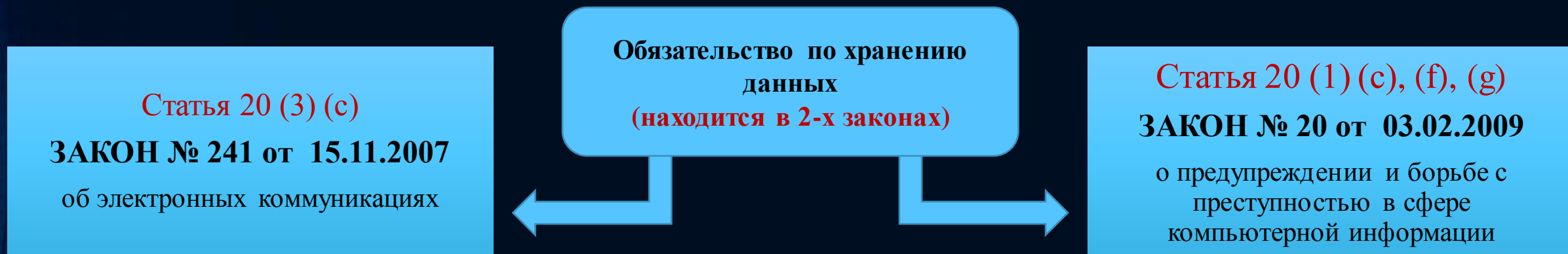
**ЗАКОН № 133 от
08.07.2011**

о защите персональных
данных

**Уголовно-
процессуальный кодекс**

№122 от 14.03.2003

(а) Обязательство по хранению данных



Общее обязательство → “хранить всю имеющуюся информацию, полученную или обработанную в процессе предоставления собственных услуг электронных коммуникаций”

Цель → идентификация источника, назначения и типа источника коммуникаций, оборудование, координаты оборудования

Сроки хранения → 6 месяцев (все что связано с интернетом)

(с) запросы компетентного органа о незамедлительном сохранении компьютерных данных или данных об информационных потоках, → не более **120 календарных дней**;

(f) данных об информационных потоках для идентификации поставщиков услуг, пользователей услуг и канала, → **180 календарных дней**;

(g) компьютерных данных, содержащихся в пакетах протоколов сети → **90 календарных дней**.

(b) Пути доступа компетентных органов (1)

**Обязательство
интернет компаний**
предоставить доступ к
данным

-Статья 20 (3) (a)
- ЗАКОН № 241 от 15.11.2007 об
электронных коммуникациях
-Статья 7 (1) (d) (2)
ЗАКОН № 20 от 03.02.2009
о предупреждении и борьбе с
преступностью в сфере
компьютерной информации

(3) Поставщики сетей и/или услуг
электронных коммуникаций независимо
от вида собственности **обязаны:**

а) представлять в соответствии с
законом уполномоченным органам,
**осуществляющим оперативно-
розыскную деятельность**, данные о
пользователях и о предоставленных им
общедоступных услугах электронных
коммуникаций;

**Доступ к хранимым
данным**
=
специальная следственная
деятельность

-Статья 132² (1) (h)
Уголовно-процессуальный
кодекс

(1) С целью раскрытия и расследования
преступлений осуществляются
следующие **специальные розыскные
мероприятия:**

h) сбор информации от поставщиков
услуг электронных коммуникаций;

(b) Пути доступа компетентных органов (2)

Компетентные органы

для проведения
специальной
следственной деятельн
ость

Статья 6 (1)

ЗАКОН № 59 от 29.03.2012
о специальной розыскной
деятельности

-Министерству внутренних дел;
-Министерству обороны;
-Нац. центру по борьбе с коррупцией;
-Службе информации и безопасности;
-Службе государственной охраны;
- Таможенной службе;
-Деп. пенитенциарных учреждений.

Типы данных

для доступа

Статья 134⁴

**Уголовно-процессуальный
кодекс**
№122 от 14.03.2003

владельцы номеров телефонов; телефонные номера; источник связи; пункт назначения связи; тип, дата, время и продолжительность сеансов связи; коммуникационное оборудование пользователя; местонахождение оборудования мобильной связи.

Метод

проверки

Статья 18 (1) 1) (h)

ЗАКОН № 59 от 29.03.2012
о специальной розыскной
деятельности

1) с разрешения судьи по уголовному преследованию, по ходатайству прокурора:

h) сбор информации от поставщиков услуг электронных коммуникаций;

II) Практика интернет-компаний

Значительные
обязательства →
значительные
потребности в срок
хранения и безопасности
для ИТ-компаний

**Обеспечение
безопасности**

**Части хранятся за
рубежом без
разрешения НЦЗПД**

*Практика местных
органов публичного
управления*
Обычное
использование,
Чрезмерный объем,
Нечеткие данные
после доступа
правоохранительных
органов

III) Защита данные в контексте сохранения

(а) Юридические гарантии

Обязанность
уничтожить
личные данные

Статья 11 (1)

ЗАКОН № 133 от 08.07.2011
о защите персональных данных

Статья 20 (3) (с)

ЗАКОН № 241 от 15.11.2007
об электронных коммуникациях

- По истечении срока хранения персональные данные подлежат уничтожению в установленном законом порядке.



- указанная информация подлежит безвозвратному уничтожению посредством автоматизированных процедур

Проверка и
рекомендации
НЦЗПД

Статья 62² (3)

ЗАКОН № 241 от 15.11.2007
об электронных коммуникациях

НЦЗПД может проверять меры [...] и может издавать рекомендации о лучших практиках в отношении уровня безопасности

Ограниченный
доступ к
персональным
данным

Статья 5 (1) (2)

ЗАКОН № 59 от 29.03.2012
о специальной розыскной
деятельности

Доступ [...] материалам дела иных лиц запрещен, за исключением:

- лиц расследующие специальное дело
- руководителя подразделения
- прокурора
- судьи по уголовному преследованию

(b) Контекст ЕС и последствия для РМ

Аннулирование **Директивы 2006/24**
→ отсутствие общей правовой базы ЕС



Соглашение об ассоциации между РМ и ЕС → адаптация
законодательства к решению **Digital Rights Ireland**

CJUE Tele2 Sverige c 21/12/2016

→ описывает ряд **общих критериев** при сохранении данных:

- не может быть наложено общие обязательства по сохранению данных
- должно быть необходимым и пропорциональным
- должно использоваться целевым образом
- должно использоваться для борьбы с серьезными преступлениями
- доступ к данным, должен быть условным
- должна существовать серия гарантий защиты данных

**Они не были учтены
в национальном
законодательстве**

ВЫВОДЫ

Значительные
юридические
обязательства для
интернет-компаний с
точки зрения
сохранения данных



(I) Трудности для
интернет-компаний,
хранить
значительные
объемы данных

Значительные
права для
правоохранительных
органов с точки зрения
доступа к этим данным



(II) Обычное
использование,
Чрезмерный объем
данных,
Нечеткие данные в
отношении будущего
использования

Наличие гарантий
защиты данных...



(III)...но не
соответствуют
критериям CJUE *Tele2
Sverige* (2016)



Контактная информация

Национальный Центр по защите Персональных Данных

- MD-2004, Республика Молдова,
- мун. Кишинэу, ул. Сергей Лазо, 48
- тел: +373-22-820801
- факс: +373-22-820807
- e-mail: centru@datepersonale.md
- www.datepersonale.md

**Спасибо за
внимание!**