ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

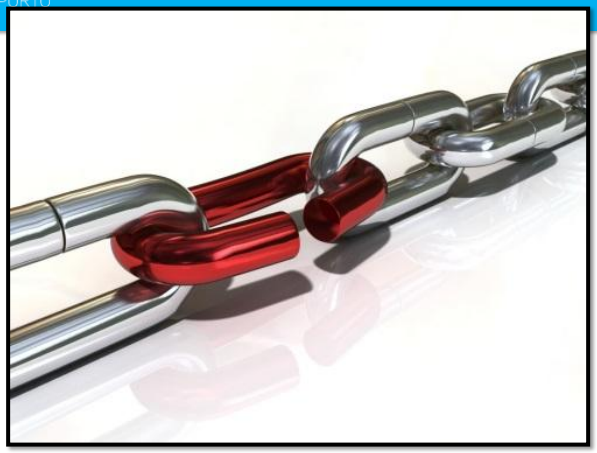
ÉTICA E LEGISLAÇÃO INFORMÁTICA

FRANCISCO MARQUES VIEIRA *fjv@estg.ipp.pt*

FMV2025

1

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO



Criminalidade Informática

Direito do Cibercrime

FMV2025

2

O que acontece

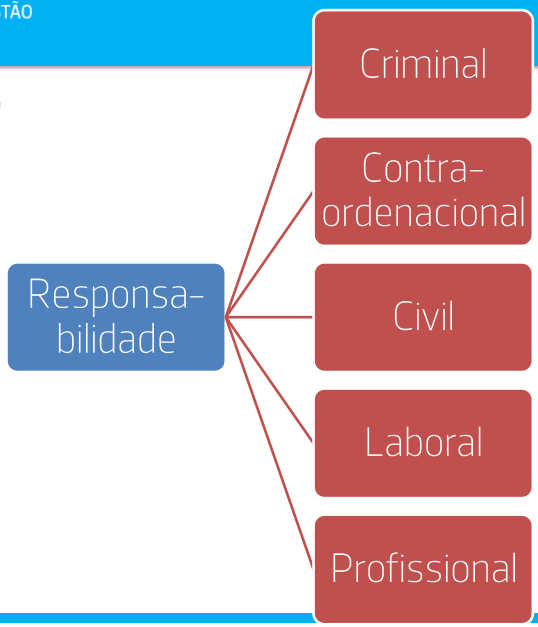
a quem

viola

a lei ou um direito ?

3

Responsabilidade



4

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Responsabilidade Criminal

Estado
- *Jus Puniendi* = Poder de Punir
- Cria, julga e aplica

Lei Penal
- Define os crimes – *tutela de bens jurídicos*
- Define as penas para cada crime

Objetivos
- Retribuição (-)
- Prevenção (+)

5

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Notícia do Crime

Legitimidade do MP

- Denúncia
- OPC
- Conhecimento próprio

Denúncia
Queixa

6

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Natureza dos Crimes

Crime Público	· Regra geral
Crime Semipúblico	· Queixa
Crime Particular	· Queixa + Constituição de Assistente + Acusação particular

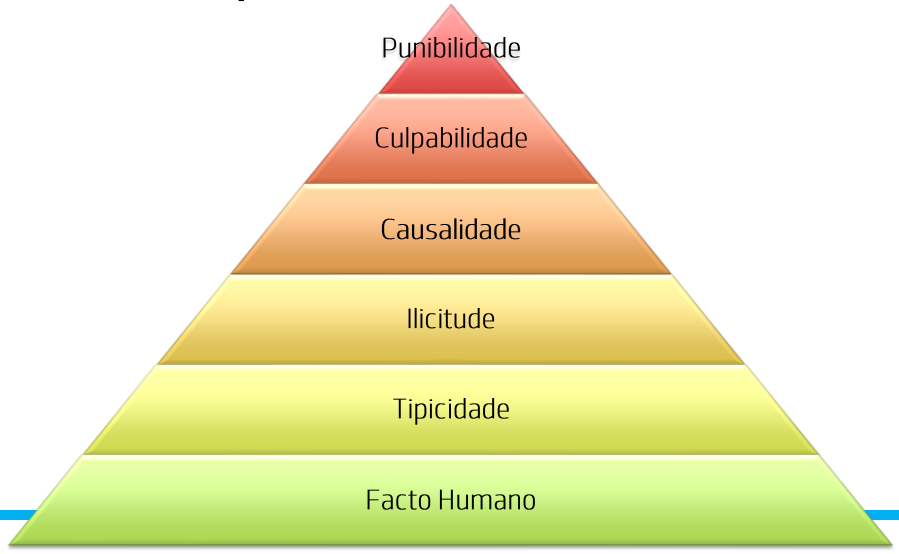
FMV2025

7

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Conceitos Essenciais

Responsabilidade Criminal



FMV2025

8

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Criminalidade Informática

- A informática levanta dois problemas essenciais ao Direito Penal:

1. Elemento potenciador da criminalidade:
   - A deslocação criminosa para a Web
   - A deslocação criminosa na Web
   - Novas técnicas de encobrimento da atividade criminosa
2. Apresenta novas realidades a proteger
   - Bens digitais (software, bases dados, etc...)
   - Sistemas informáticos

FMV2025

9

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Criminalidade Informática

FMV2025

10

Novos Bens Jurídicos Digitais

- Bens protegidos pelo Direito Penal clássico ou necessidade de nova categoria?
  - crimes informáticos em sentido estrito ou
  - crimes informáticos propriamente ditos ou
  - crime informático-digital próprio ou "puro"

Criminalidade Informática

- Criminalidade informática engloba duas realidades distintas:

1. Os crimes em que a informática é apenas um novo meio para a prática de crime não especificamente previsto para o ambiente digital
2. Os crimes em que a informática é um elemento integrador do tipo legal ou o bem protegido.

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Criminalidade Informática

Criminalidade informática em sentido amplo

Toda a realidade associada aos crimes praticados por meios informáticos.

Inclui os crimes cuja ofensa é passível de se consumar em ambiente digital, a saber:

- Por violação de propriedade intelectual (previstos no CDADC ou no CPI)
- Por violação de Direitos de Personalidade (sejam os previstos no CP – com a honra ou a difamação – sejam os previstos em legislação relativa à tutela de dados pessoais)

Mas também aqueles em que apenas os atos instrumentais ou preparatórios são praticados em ambiente digital.

E também os crimes informáticos em sentido estrito – *a seguir*

13

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Criminalidade Informática

Criminalidade informática em sentido estrito

Aquela em que a informática é uma elemento integrador do tipo legal ou do bem protegido

- Aquela em que os atos que integram o crime estão especificamente previstos para o ambiente digital
  - Ex.: a "Burla Informática" ou a "Falsidade Informática"
- Os crimes em que o bem jurídico ofendido é um bem digital.
  - Ex.: a "reprodução ilícita de software" ou a "sabotagem informática"

14

Criminalidade Informática

- Código Penal
- Lei do Cibercrime
  - Lei 109/2009, de 15 de Setembro
- Leis extravagantes
  - CDADC
  - DL 122/00
  - Lei 58/2019 – lei de execução do RGPD
  - Lei 59/2019

15

Código Penal

- introdução na habitação de outra pessoa ou nela permanecer depois de intimado a retirar-se;
- intenção de perturbar a vida privada, a paz e o sossego de outra pessoa, telefonar para a sua habitação ou para o seu telemóvel

Crime contra a reserva da vida privada

Art. 190.º CP

16

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Código Penal

- Com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:
  - Intercetar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio eletrónico ou faturação detalhada;
  - Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objetos ou espaços íntimos;
  - Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
  - Divulgar factos relativos à vida privada ou a doença grave de outra pessoa;

Crime devassa da vida privada

Art. 192.º CP

17

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Código Penal

- disseminar ou contribuir para a disseminação de imagens, fotografias ou gravações que devassem a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual

Crime de devassa através de meio de comunicação social, da internet ou de outros meios

Art. 193.º CP

18

Código Penal

- abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido

Crime de violação de correspondência ou telecomunicações

Art. 194.º CP

19

Código Penal

- Gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas;
- Fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado

Crime de gravações e fotografias ilícitas

Art. 199.º CP

20

Código Penal

- intenção de obter enriquecimento ilegítimo ou causar prejuízo patrimonial
- interferir no tratamento de dados ou em programa informático..... ...
- Ou usar programas ou dispositivos eletrónicos para diminuir, alterar ou impedir o normal funcionamento de serviços de telecomunicações

Crime de burla informática e nas comunicações

Art. 221.º CP

21

Os tipos legais de crimes na Lei do Cibercrime

CARACTERIZAÇÃO

22

Os crimes da Lei do Cibercrime

- Crimes que tutelam a "confiança" nos sistemas informáticos:
  - «Falsidade informática» – art. 3.º,
  - «Sabotagem informática» – art. 5.º
  - «Acesso ilegítimo» – art. 6.º,
  - «Interceção ilegítima» – art. 7.º,
- Crimes que tutelam a "propriedade" de bens digitais:
  - «Dano relativo a programas ou outros dados informáticos» art. 4.º,
  - «Reprodução ilegítima de programa protegido» – art. 8.º.

23

Os crimes da Lei do Cibercrime

- Ordem de estudo:

I. «Acesso ilegítimo» – art. 6.º – por muitos visto com um crime preliminar ou precursor de outros ilícitos informáticos.

II. «Dano relativo a programas ou outros dados informáticos» art. 4.º – também ele um crime cujo ato material iremos encontrar em outros ilícitos e que por isso se encontra muitas vezes em concurso com outros crimes informáticos.

III. Abordaremos de seguida os demais crimes previstos na Lei do Cibercrime por ordem de previsão legal:
  - «Falsidade informática» – art. 3.º,
  - «Sabotagem informática» – art. 5.º
  - «Interceção ilegítima» – art. 7.º,
  - «Reprodução ilegítima de programa protegido» – art. 8.º.

24

Crime de Acesso Ilegítimo art. 6.º LC

Os crimes da Lei do Cibercrime

25

Crime de acesso ilegítimo

- Elementos objetivos do tipo legal:
  - "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele,"
  - "de qualquer modo aceder a um sistema informático"
- Elementos subjetivos do tipo legal:
  - Dolo genérico (art. 13.º CP).

26

Crime de acesso ilegítimo

- Bem protegido:
  - Essencialmente segurança dos sistemas informáticos
  - Há quem sustente que indiretamente tutela outros valores por impedir que o agente fique em circunstância de lesar outros bens jurídicos – por exemplo, dados pessoais ou património
- Tipo de crime:
  - O procedimento criminal dependerá de queixa, sendo um crime semipúblico.
  - Exceto nos casos previstos no números 2, 3 e 5 do artigo 6.º, em que se dispensa a necessidade de queixa, sendo então um crime público.
- Atuações puníveis:
  - Consumação: a moldura penal na sua forma simples é de pena de prisão até 1 ano ou pena de multa até 120 dias.
  - No entanto, o n.º 6 do artigo 6.º da Lei 109/2009 prevê que expressamente a punibilidade da tentativa

27

Crime de acesso ilegítimo

Inclui-se na previsão legal deste crime (n.º 2):

- "quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas". *(n.º 2 do art. 6.º da Lei 109/2009)*
- Neste caso o crime apenas será punível na sua forma consumada (art. 6.º n.º 6 in fine Lei 109/2009).
- Ainda assim permanece um crime de perigo pois não requer a existência de um dano ou efetivo "acesso ilegítimo".

28

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Crime de acesso ilegítimo

Sustenta-se que este crime visa, indiretamente, criar uma "barreira para evitar a prática de outros ilícitos mais graves"

- Desde logo, os crimes relativos à tutela da privacidade (dados pessoais, imagem, intimidade da vida privada)
- Mas também crimes tipicamente informáticos como:
  - "dano relativo a dados informáticos"
  - "sabotagem informática"
  - "falsidade informática"
- Nestes casos o valor tutelado pelo "acesso ilegítimo" é por regra autónomo do valor tutelado por esses segundos crimes, sendo eles punidos em concurso real.

29

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Crime de Dano Informático
Art. 4.º LC

Os crimes da Lei do Cibercrime

33

Crime de Dano Informático

- Elementos objetivos do tipo legal:
  - "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele,
  - "apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso"
- Elemento subjetivo do tipo:
  - Dolo genérico (art. 13.º CP)

Crime de Dano Informático

- Bem protegido:
  - Integridade dos dados informáticos
  - Indiretamente também se defende que tutela o património digital do lesado
- Tipo de crime:
  - o procedimento criminal depende de queixa, sendo um crime semipúblico
- Atuações puníveis:
  - Apesar de estar previsto para este crime, na sua forma simples, uma moldura penal de pena de prisão até 3 anos ou pena de multa, o n.º 2 do artigo 4.º prevê expressamente a punibilidade da tentativa.

Crime de Dano Informático

- Inclui-se na previsão legal deste crime:
- "quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número" *(n.º 3 do art. 4.º da Lei 109/2009).*
- Criminalização da difusão de vírus,
- É um crime de perigo, pois estes atos são penalizados independentemente de esses danos se virem a efetivar ou não

36

Crime de Dano Informático

- Veremos adiante que a particularidade do crime de dano é que o seu ato material essencial
  - "apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso" –
- constitui o ato material essencial de outros tipos legais de crimes informáticos (como a sabotagem informática e a falsificação informática) que se distinguem do dano essencialmente pelo distinto efeito "lesivo" ou "jurídico" do ato de "dano".
- Teremos pois de analisar neste caso com mais cuidado a possibilidade de concurso real e ou aparente de crimes.

38

Crime de Falsidade Informática Art. 3.º LC

Os crimes da Lei do Cibercrime

39

Crime de Falsidade Informática

- Elementos objetivos do tipo legal:
  - "introduzir, modificar, apagar ou suprimir dados informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados"
  - "produzindo dados ou documentos não genuínos,"
- Elementos subjetivos do tipo legal:
  - "intenção de provocar engano nas relações jurídicas"
  - "com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem"

40

Crime de Falsidade Informática

- Bem protegido:
  - a segurança das relações jurídicas
  - a confiança nos documentos eletrónicos / integridade dos SI
- Tipo de crime:
  - Não se prevendo a necessidade de queixa-crime para se iniciar o procedimento criminal, mantém-se como um crime público
- Atuações puníveis:
  - Estando previsto para este crime, na sua forma simples, uma moldura penal de pena de prisão até 5 anos ou multa de 120 a 600 dias, teremos de concluir que, por aplicação do disposto no artigo 23.º do Código Penal o crime de Falsidade Informática será punido na sua forma tentada.

41

Crime de Sabotagem Informática Art. 5.º LC

Os crimes da Lei do Cibercrime

46

O Crime de Sabotagem informática

Elementos Objetivos do tipo legal:

- "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele"
- "entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos"
- ou
- "de qualquer outra forma de interferência em sistema informático"

Elementos Subjetivos do tipo legal:

- Dolo genérico (art. 13.º CP)

47

O Crime de Sabotagem informática

- Bem protegido:
  - a segurança dos sistemas e comunicações eletrónicas
- Tipo de crime:
  - não depende de queixa para o prosseguimento do procedimento criminal, sendo um crime público
- Atuações puníveis:
  - Estando previsto para este crime, na sua forma simples, uma moldura penal de pena de prisão até 5 anos ou multa até 600 dias, teremos de concluir que, por aplicação do disposto no artigo 23.º do Código Penal, o mesmo será punido na sua forma tentada.

48

O Crime de Sabotagem informática

Inclui-se ainda na previsão legal deste crime:

- "quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas" *(n.º 2 do art. 5.º da Lei 109/2009)*.

  – É neste caso um crime de perigo, pois estes atos passam a ser penalizados independentemente de esses danos se virem a efetivar ou não.

Crime de Interceção Ilegítima Art. 7.º LC

Os crimes da Lei do Cibercrime

Crime de Interceção ilegítima

Elementos Objetivos do tipo legal:

- "sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele,"
- "através de meios técnicos"
- "intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes"

Elementos Subjetivos do tipo legal:

- Dolo genérico (art. 13.º CP)

52

Crime de Interceção ilegítima

- Bem protegido:
  - a segurança e privacidade das comunicações electrónicas
- Tipo de crime:
  - não depende de queixa para o prosseguimento do procedimento criminal, sendo um crime público
- Actuações puníveis:
  - A moldura penal prevista para este crime é de pena de prisão até 3 anos ou pena de multa. O n.º 2 do artigo prevê igualmente a punibilidade da tentativa.

53

Crime de Interceção ilegítima

Inclui-se ainda na previsão legal deste crime:

- "quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas" *(n.º 23do art. 7.º da Lei 109/2009)*.

  – Temos assim também neste caso um crime de perigo pois não requer a existência de um dano ou efetiva "intercepção ilegítima".

Crime de Reprodução Ilegítima de Programa
Art. 8.º LC

Os crimes da Lei do Cibercrime

Crime de Reprodução ilegítima de programa protegido

Elementos Objetivos do tipo legal:

- Quem, não estando para tanto autorizado = *ilegitimamente*
- reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei

Elementos Subjetivos do tipo legal:

- Dolo genérico (art. 13.º CP)

Crime de Reprodução ilegítima de programa protegido

- Bem protegido:
  - o direito do Autor sobre o programa de computador, mas também a proteção da propriedade intelectual como elemento de desenvolvimento económico do Estado.
- Tipo de crime:
  - Este crime não depende de queixa, sendo um crime público
- Atuações puníveis:
  - o n.º 3 deste artigo 8.º estabelece que a tentativa será também punida.

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

O estranho caso do tipo legal "oculto" no art. 8.º

O n.º 2 deste artigo 8.º da LC é um caso verdadeiramente estranho na legislação penal portuguesa.

Dispõe este n.º 2 que:

"Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia."

- Desde logo, porque as topografias de semicondutores não vêm referidas na epígrafe do artigo,
- nem têm uma relação direta e necessária com os programas de computador para integrar no seu objeto de tutela... exceto quando elas próprias são a forma de expressão de um "firmware"...

62

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

O estranho caso do tipo legal "oculto" no art. 8.º

Mas também porque...

- As "topografias de semicondutores" encontram a sua definição e no Código da Propriedade Industrial (CPI).

«Topografia de um produto semicondutor é o conjunto de imagens relacionadas, quer fixas, quer codificadas, que representem a disposição tridimensional das camadas de que o produto se compõe, em que cada imagem possua a disposição, ou parte da disposição, de uma superfície do mesmo produto, em qualquer fase do seu fabrico» (art. 154.º CPI)

- Sendo que o artigo 318.º do CPI já pune com «com pena de prisão até três anos ou com pena de multa até 360 dias quem, sem consentimento do titular do direito» fabricar, aplicar, importar ou exportar topografias de semicondutores protegidas. Punindo o Art. 321.º CPI a venda e ocultação deste produtos.

FMV2025

63

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

O estranho caso do tipo legal "oculto" no art. 8.º

- Parece-nos que este o crime previsto no artigo 8.º n.º 2 da LC se encontra totalmente "consumido" pelos crimes previstos no artigo 318.º e 321.º do CPI.
- Sendo que esta sobreposição se vem repetindo quer na evolução legislativa da Lei da Criminalidade Informática (Lei 109/91, de 17/08) para a Lei do Cibercrime) para a Lei do Cibercrime (Lei 10972009, de 15/09); quer nas sucessivas alterações ao Código da Propriedade Industrial.
- Não vislumbramos qual seja o benefício desta "duplicação" de tipos legais.

64

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

A Tutela Penal da Lei n.º 58/2019, de 8 de agosto

Tipos de legais de crimes sobre dados pessoais:

- Art. 46.º – Crime de utilização de dados de forma incompatível com a finalidade da recolha
- Art. 47.º – Crime de acesso indevido
- Art. 48.º – Crime de desvio de dados
- Art. 49.º – Crime de viciação ou destruição de dados
- Art. 50.º – Crime de inserção de dados falsos
- Art. 51.º – Crime de violação do dever de sigilo
- Art. 52.º – Crime de desobediência

65

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

A Tutela Penal da Lei n.º 58/2019, de 8 de agosto

- Bem jurídico protegido:
  - Dados pessoais
- Tipos de crime:
  - Públicos – não depende de queixa
  - Dolosos – não se prevê a negligência (art. 13.º CP)
  - Negligentes
    - art. 49.º (viciação ou destruição de dados) agravado admite negligência
    - art. 50.º (inserção de dados falsos) agravado admite negligência
    - art. 51.º (violação do dever de sigilo) admite negligência
- Atuações puníveis:
  - O art. 53.º prevê a punibilidade da tentativa em todos os crimes da Lei n.º 58/2019.

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Artigo 46.º

Crime de utilização de dados de forma incompatível com a finalidade da recolha

- Elementos objetivos do tipo legal:
  - "Quem utilizar dados pessoais de forma incompatível com a finalidade determinante da recolha".
- Pena:
  - pena de prisão até um ano ou com pena de multa até 120 dias
  - a pena é agravada para o dobro nos seus limites no *caso de dados sensíveis*.

Artigo 47.º

Crime de acesso indevido

- Elementos objetivos do tipo legal:
  - "Quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais"
- Pena:
  - Pena de prisão até 1 ano ou com pena de multa até 120 dias.
  - Pena agravada para o dobro:
    - No caso de dados sensíveis
    - Se houver violação de regras de segurança
    - Se houver benefício ou vantagem patrimonial

Artigo 48.º

Crime de desvio de dados

- Elementos objetivos do tipo legal:
  - Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento
- Pena:
  - pena de prisão até 1 ano ou com pena de multa até 120 dias.
  - Pena agravada para o dobro:
    - No caso de dados sensíveis
    - Se houver violação de regras de segurança
    - Se houver benefício/vantagem patrimonial

Artigo 49.º

Crime de viciação ou destruição de dados

- Elementos objetivos do tipo legal:
  - Quem, sem a devida autorização ou justificação, apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afetando o seu potencial de utilização
- Pena:
  - pena de prisão até 2 anos ou com pena de multa até 240 dias.
  - A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.

Artigo 50.º

Crime de inserção de dados falsos

- Elementos objetivos do tipo legal:
  - Quem inserir ou facilitar a inserção de dados pessoais falsos
- Elementos subjetivos do tipo legal:
  - com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo
- Pena:
  - pena de prisão até 2 anos ou com pena de multa até 240 dias.
  - Agravada para o dobro se da inserção resultar um prejuízo efetivo

Artigo 51.º

Crime de violação do dever de sigilo

- Elementos objetivos do tipo legal:
  - Quem, obrigado a sigilo profissional nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais
- Pena:
  - prisão até 1 ano ou multa até 120 dias.
  - Agravada para o dobro se o agente:
    - For trabalhador em funções públicas ou equiparado, nos termos da lei penal;
    - For encarregado de proteção de dados;
    - Intenção de obter qualquer vantagem patrimonial ou benefício ilegítimo;
    - Puser em perigo a reputação, a honra ou a intimidade da vida privada

Artigo 52.º

Crime de desobediência

- Elementos objetivos do tipo legal:
  - Quem não cumprir as obrigações previstas no RGPD e Lei 58/2019
  - depois de ultrapassado o prazo que tiver sido fixado pela CNPD para o respetivo cumprimento
- Pena:
  - prisão até 1 ano ou com multa até 120 dias
  - Agravada para o dobro se, depois de notificado para o efeito, o agente:
    - Não interromper, cessar ou bloquear o tratamento ilícito de dados;
    - Não proceder ao apagamento ou destruição dos dados quando legalmente exigível, ou findo o prazo de conservação fixado nos termos da presente lei; ou
    - Recusar, sem justa causa, a colaboração que lhe for exigida nos termos do artigo 8.º da presente lei.

A Tutela Penal da Lei n.º 59/2019, de 8 de agosto

Tutela "paralela" à da Lei 58/2019, mas relativa ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais

- Art. 53.º – Crime de acesso indevido aos dados
- Art. 54.º – Crime de desvio de dados
- Art. 55.º – Crime de utilização de dados de forma incompatível com a finalidade da recolha
- Art. 56.º – Crime de Interconexão ilegal de dados
- Art. 57.º – Crime de viciação ou destruição de dados
- Art. 58.º – Crime de violação do dever de sigilo
- Art. 59.º – Crime de desobediência qualificada
- Art. 60.º – Crime de inserção de dados falsos

As disposições processuais da Lei do Cibercrime

Medidas relativas à pesquisa e retenção de dados informáticos

- O artigo 11.º prevê que as medidas de pesquisa e retenção da dados informáticos sejam utilizáveis na investigação de:
  - Crimes previstos na própria Lei do Cibercrime;
  - Crimes cometidos por meio de sistema informático; e
  - Em relação aos quais seja necessário proceder à recolha de prova de suporte eletrónico
- São assim medidas de aplicação geral a toda a criminalidade informática em sentido amplo!

Medidas relativas à pesquisa e retenção de dados informáticos

- As medidas previstas para o combate à criminalidade informática em sentido amplo são:
  - a "preservação expedita de dados" – artigo 12.º
  - - a "revelação expedita de dados" – artigo 13.º
  - - a "injunção para apresentação ou concessão de acesso a dados" – artigo 14.º
  - - a "pesquisa de dados informáticos" – artigo 15.º
  - - a "apreensão de dados informáticos" – artigo 16.º
  - e a apreensão de correio eletrónico e registos de comunicações de natureza semelhante – artigo 17.º

Medidas especiais de aplicação limitada

- O artigo 18.º prevê a interceção de comunicações eletrónicas:
  - em processos de investigação relativos a crimes previstos na lei do cibercrime
  - ou cometidos por meio de um sistema informático (ou seja na criminalidade informática em sentido lato)
  - e ainda para crimes em que a lei processual penal geral admita as escutas telefónicas (artigo 187.º do Código de Processo Penal). ;

Medidas especiais de aplicação limitada

- O artigo 19.º prevê o recurso a ações encobertas no decurso de inquérito :
  - Em crimes previstos na lei do cibercrime
  - Em crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos
  - ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras,
  - bem como os crimes contra obras protegidas por direito de autor (título IV do CDADC).

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Cooperação internacional – Medidas institucionais

- Âmbito (art. 20.º LC):
  - Limita a cooperação à investigação de crimes "relacionados com sistemas ou dados informáticos".
- Ponto de contacto (art. 21.º LC):
  - Cria o ponto de contrato 24/7 imposto pelo artigo 35.º da Convenção de Budapeste

80

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Cooperação internacional – Medidas institucionais

- Preservação e revelação expeditas de dados informáticos (art. 22.º e 23.º LC):
- Acesso a dados informáticos (art. 24.º e 25.º LC):
- Interceção de comunicações (art. 26.º LC):

81