LEIS E REGULAMENTOS QUE REGEM A CIBER-SEGURANÇA

Co-funded by the Erasmus+ Programme of the European Union

Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões.

LECTURAS

1. Introdução ao tema, sistema de direito, norma jurídica, direito e internet
2. Responsabilidade no ciberespaço
3. Base jurídica da actividade do ISP (Internet service provider)
4. A ciber-segurança e a sua regulamentação legal
5. ISMS
6. Protecção de dados pessoais no ciberespaço
7. Privacidade e segurança nas TIC, protecção de dados no ciberespaço

WORKSHOPS

1. Definição do âmbito da lei no ciberespaço (limites, possibilidades, etc.)
2. Responsabilidade privada e pública pelas acções do utilizador ou empresa no ambiente online
3. Características e definição de cada FSI e dos seus direitos e obrigações em relação à ciber-segurança
4. ISMS e a relação com a lei da ciber-segurança
5. Aquisição de direitos e obrigações básicos para assuntos individuais à Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação em toda a União, também da legislação nacional.
6. Aplicação dos direitos e obrigações decorrentes da GDPR no ciberespaço
7. Análise prática das condições contratuais com os ISPs em relação à protecção da privacidade

Tabela de Conteúdos

1. Introdução ao tema, sistema de direito, norma jurídica, direito e internet

A lei é um dos instrumentos mais importantes para estabilizar as relações sociais e regular a sociedade.

A lei é necessária e actualmente insubstituível porque, onde existe uma sociedade, existe lei. A sociedade não é capaz de suportar sem ordem e sem regras. Como tal, o direito reduz significativamente o grau de caos (entropia) na sociedade e estabiliza as relações.

Tudo o que foi dito acima é verdade, mas apenas se a lei for respeitada e se a própria lei for estável (pelo menos relativamente).

A lei, tal como a sociedade, está a evoluir e a mudar.

A lei é um conjunto de regras de conduta geralmente vinculativas aceites pela sociedade, definidas por um Estado ou organismos autorizados pelo Estado. Para que a lei seja sustentável, deve ser exequível. A lei sem a condição de aplicabilidade ainda é lei, mas na realidade é antes um conjunto de recomendações que cada um decide por si se deve ou não respeitar.

Para que um cidadão ou uma entidade sujeita a uma lei possa exercer os seus direitos ou protegê-los eficazmente e estar consciente das suas próprias responsabilidades, que estão intimamente ligadas aos direitos, precisa de ter pelo menos um conhecimento mínimo das disposições básicas do sistema jurídico.

Na sociedade actual, a lei pode ser caracterizada como um sistema de normas legais relativamente bem definido, garantido pelo poder do Estado e protegido pela aplicação da lei pelo Estado. Para que uma pessoa singular ou colectiva possa exercer ou proteger eficazmente os seus direitos, bem como estar ciente das suas obrigações ao abrigo destes direitos, é essencial que tenha pelo menos um conhecimento mínimo das disposições básicas do sistema jurídico.

O conceito real da lei é relativamente difícil de definir, pois trata-se de um fenómeno multidisciplinar e não pode ser definido por uma única definição:

- **lei natural** *(ius naturale)*. Ela existe independentemente do Estado. Tem origem e desenvolve-se na sociedade. Em geral, compreende um conjunto de princípios que correspondem ao nível alcançado de desenvolvimento da sociedade.
- **lei positiva** *(ius pozitivum)*. Esta lei é estabelecida por um Estado ou um sistema de poder. A lei positiva é, portanto, pré-determinada. Consiste em regras previsíveis que são aplicadas, ou seja, onde a infracção é punida.
- **lei** Entendemos a lei (ou lei objectiva) como um conjunto de normas legais como regras de conduta geralmente vinculativas estabelecidas ou reconhecidas e aplicadas pelo Estado.
- **direito** "Direito" significa a possibilidade de conduta de pessoas colectivas garantida por uma norma legal. Um direito corresponde normalmente a uma obrigação legal de outra entidade jurídica. A afirmação de uma entidade de que "é meu direito" corresponde à lei neste sentido, por exemplo.

1.1 Norma legal

Uma norma jurídica é um elemento essencial de um Estado baseado no Estado de direito.

Uma norma jurídica representa uma regra de conduta geralmente vinculativa que regula os direitos e obrigações das entidades. Esta norma de conduta é expressa numa forma jurídica especial reconhecida pelo Estado (ou pela União Europeia), e a sua observância é assegurada pela execução estatal.

A definição acima de norma legal resulta em duas características obrigatórias, que são mais especificadas. Estas características são:

1. **Formal**

   Do ponto de vista do cumprimento da característica formal de uma norma legal, é necessário que uma norma legal seja emitida por uma entidade autorizada e, ao mesmo tempo, que o método de publicação legalmente prescrito seja satisfeito.

2. **Material**

   As características materiais de uma norma legal incluem:

   - regulação - regula as relações sociais,
   - juridicamente vinculativo - a regra de conduta regula as relações sociais com efeitos vinculativos,
   - generalidade - em termos do objecto da legislação, bem como do objecto da norma legal,
   - aplicabilidade por poder estatal - "aplicação da lei pelo Estado" no caso de a lei não ser respeitada.

A **estrutura** padrão **de uma norma legal consiste em três partes**, que são a **hipótese, a disposição** e a **sanção**.

A hipótese estabelece as condições sob as quais uma norma legal é implementada. A hipótese, em particular, define os factos, entidades e objectos jurídicos de uma norma a que os direitos e obrigações se relacionam.

A disposição representa a sua própria regra de conduta ao determinar e concretizar que direitos e obrigações surgem e a quem, no caso de ocorrerem as condições declaradas na hipótese.

A sanção é uma expressão das consequências de uma violação de uma obrigação legal decorrente da disposição de uma norma legal.

Divisão das normas jurídicas

As normas legais podem ser divididas de acordo com vários critérios. Estes são especificamente:

1. *A natureza das regras estabelecidas pela norma legal.* De acordo com a natureza das regras, as normas legais dividem-se em:

- Dispositivo. Uma norma jurídica dispositiva não estipula uma regra de conduta fundamental, ou estipula apenas como uma possibilidade. É deixado ao critério dos destinatários a definição das regras. Se os destinatários não o fizerem, as disposições da norma servem de guia para que o juiz saiba como decidir. As normas de dispositivos são sobretudo aplicadas em direito civil ou em relações de direito civil, o que permite uma maior variabilidade na solução de várias situações (auto-regulação).
- Cogent (categórico). Uma norma jurídica convincente estipula uma regra de conduta vinculativa. Não deixa espaço para a vontade do destinatário.

2. *Palavras.* De acordo com a redacção, as normas legais estão divididas em:

- Entidadetidade. Estas normas legais formulam explicitamente apenas os direitos.
- Encadernação. Estas normas legais formulam explicitamente uma obrigação, quer sob a forma de uma ordem, quer sob a forma de uma proibição.

3. *Estatuto das entidades.* De acordo com o estatuto das entidades, as normas legais estão divididas em:

- Público. Estas normas legais aplicam-se onde o poder público é exercido. O poder público é exercido pelo Estado através dos gabinetes do poder legislativo, executivo e judicial. Vemos o direito público como a área do direito em que as relações se baseiam nas desigualdades das partes envolvidas, onde se representa o poder público actuando contra pessoas privadas com ordens, proibições e execução.

- Privado. Estas normas legais aplicam-se no domínio do direito privado, ou seja, onde as entidades actuam em posição de igualdade, e nenhuma delas pode decidir com autoridade sobre os direitos e obrigações da outra. As entidades regulam os seus direitos e obrigações mútuos através de contratos e acordos.

4. *Objecto de regulamentação.* De acordo com o objecto de regulamentação, as normas legais estão divididas em:

- Internacional. Estas normas legais regulam as relações entre Estados ou os seus habitantes, possivelmente a nível da União Europeia.
- Nacional. As normas jurídicas nacionais regulam as relações entre entidades dentro de uma jurisdição de um determinado Estado ou normalmente dentro do seu território.

5. *Método da legislação.* De acordo com o método da legislação, as normas legais estão divididas em:

- Direito substantivo. Estas normas jurídicas definem as relações jurídicas em geral e estabelecem os direitos e obrigações das entidades.
- Direito processual. Estas normas legais regulam o procedimento das autoridades públicas na aplicação das normas de direito substantivo, o que pode resultar na emissão de um acto público.

6. *Âmbito de aplicação da legislação.* De acordo com o âmbito da legislação, as normas legais estão divididas em:

- Generalidades. Estas normas legais afectam todo um território de um Estado ou da União Europeia. Além disso, aplicam-se a todas as entidades sem limite de âmbito temporal.
- Especial. Estas normas legais funcionam apenas num determinado território. Caso contrário, só se aplicam a uma determinada categoria de entidades ou durante um determinado período de tempo.

Eficácia das normas legais

A eficácia de uma norma legal significa que os destinatários em questão têm direitos e obrigações decorrentes da mesma. O pré-requisito para a eficácia de uma norma jurídica é a sua validade. Isto significa que uma norma jurídica não pode entrar em vigor antes do dia da sua validade. No entanto, uma norma jurídica pode entrar em vigor mais tarde. Assim, pode decorrer um certo período entre o dia em que uma norma legal se torna válida e o dia em que entrou em vigor (o chamado *vacatio legis*). Este período destina-se a permitir que os destinatários de uma norma jurídica se familiarizem com a norma legal e se adaptem à mesma. A data de entrada em vigor é normalmente indicada na última disposição da norma jurídica.

Exemplos da lei que nos rodeia:

- Contrato de compra
- Contrato de trabalho
- Acordo de empréstimo
- Contrato de trabalho / contrato de trabalho / contrato de trabalho
- Contrato para a prestação de serviços de consultoria
- Contrato de licença

- Contrato de gestão
- Acordo de Confidencialidade
- Acordo sobre a venda de uma participação comercial
- Torres civis (difamação, violação de contrato)
- Crimes (por exemplo, roubo, fraude, violação de direitos de autor, etc.)

1.2 A relação entre a lei e o ciberespaço

Muito tem sido publicado sobre a relação entre a lei e as novas tecnologias, especialmente a Internet, incluindo as suas mudanças e transformações. Mas muitas questões-chave continuam por resolver, e muitos outros problemas estão apenas na fase da sua identificação ou análise. No entanto, embora a procura de soluções razoáveis esteja no bom caminho nos melhores casos, por vezes não há solução à vista. A Internet é, sem dúvida, um fenómeno *sui generis.* Como tal, não é autónoma, mas é dirigida principalmente através da regulação da conduta dos seus utilizadores.

A lei é uma das suas possíveis regulamentações sob a forma de construções normativas imperfeitas, onde se aplica mais do que em qualquer outro lugar que entre a conduta na realidade, ou seja, o que é realmente realizado no ambiente da Internet, e a conduta normativa, ou seja, o que deveria ser (pela vontade do regulador e a nossa), não se equipara. A realidade da Internet e os seus regulamentos normativos são, portanto, duas categorias relativamente separadas. Este pressuposto também não será posto em causa nesta publicação. Pelo contrário, será um dos seus pilares.

A maioria dos problemas jurídicos relacionados com a Internet devem ser considerados no contexto jurídico e tecnológico global, e não apenas na perspectiva de fórmulas estabelecidas ou na perspectiva de disciplinas jurídicas individuais *per se*.[1]

[1] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praga: CZ.NIC, 2013. ISBN 978-80-904248-7-6 p. 25

2. Responsabilidade no ciberespaço

2.1 Ciberespaço

"Uma alucinação consensual vivida diariamente por milhares de milhões de operadores legítimos, em todas as nações, por crianças a quem são ensinados conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz que se estendem no não-espaço da mente, clusters e constelações de dados. Como as luzes da cidade, a recuar..."

William Gibson: Neuromancer (1984)

O ciberespaço é uma caixa de areia metafórica onde nos movemos, mas é também um elemento chave na definição de segurança cibernética. Para se poder definir o ciberespaço, é essencial definir o conceito de Internet, que lhe diz directamente respeito.

O início global da Internet, que é uma base material necessária do ciberespaço, remonta aos anos 50. Nessa altura, foram construídas e testadas redes de computadores interligados, principalmente para fins de investigação científica e militar. Embora a Internet tenha sido construída sobre as bases das redes ARPANET e NSFNET[2] , ninguém é actualmente proprietário da Internet, e não existe nenhuma autoridade ou instituição central para a gerir. *"No entanto, existem instituições que desempenham um papel significativo no funcionamento e desenvolvimento futuro da Internet. Em primeiro lugar, mencionemos a Sociedade da Internet (ISOC), que reúne os utilizadores da Internet. A ISOC tem duas componentes principais: o Conselho de Actividades da Internet (IAB) e a Task Force de Engenharia da Internet (IETF). Estes dois componentes trabalham com as empresas informáticas mais importantes para criar as normas necessárias para o desenvolvimento futuro da Internet*" [3]

A ICANN[4] (Internet Corporation for Assigned Names and Numbers) tem uma posição soberana dentro da Internet. O âmbito de actividades desta associação inclui o estabelecimento de regras para o funcionamento do sistema de nomes de domínio. Hoje em dia, porém, os ISP estão a ganhar cada vez mais proeminência, e a desempenhar um papel cada vez mais importante.[5]

A base material da Internet é a sua rede de base, que conduz um sinal (dados) através do ar, cabos ou outros meios de transmissão. Em termos técnicos, significa a rede informática distribuída mundialmente, composta por redes individuais mais pequenas que estão interligadas através de protocolos Internet (IPs) e permitem assim a comunicação, transferência de dados, informação e prestação de serviços entre entidades. Isto cria de facto um sistema dinâmico, em constante mudança e evolução ligado ao hardware, mas ao mesmo tempo, cria um ciberespaço difícil de definir e virtualmente ilimitado. Pode-se dizer que o ciberespaço é uma realidade virtual que é efectivamente ilimitada. Contudo, esta realidade virtual depende completamente da base material, ou seja, das tecnologias encontradas no mundo real. Isto cria um paradoxo interessante que permite a existência de meios intangíveis (ciberespaço) capazes, devido à distribuição de meios tangíveis (elementos de rede, sistemas informáticos individuais, armazenamento em nuvem, serviços interligados, etc.) de se adaptarem e alterarem em caso de danos nos meios materiais, mas em caso de colapso completo do meio material (ou de todos os seus componentes), ocorrerão danos irreversíveis ou a extinção do ciberespaço enquanto tal.

---

[2] Cf. *Internet History of 1980s.* [em linha]. [cit. 07/06/2016]. Disponível a partir de: http://www.computerhistory.org/internethistory/1980s/

[3] *Internet, připojení k němu a možný rozvoj (Část 2 - Historie a vývoj Internetu).* [online]. [cit.10/02/2008]. Disponível a partir de: http://www.internetprovsechny.cz/clanek.php?cid=163

[4] Para mais detalhes, ver https://www.icann.org/

[5] ISP - Fornecedor de Serviços Internet.

O ciberespaço também pode ser definido como um espaço de actividades cibernéticas, ou como um espaço criado pelas tecnologias de informação e comunicação onde é criado um mundo virtual (ou espaço) paralelo ao espaço real.

O conceito de ciberespaço começou a tornar-se mais amplamente conhecido após a declaração de John Barlow (fundador da Electronic Frontier Foundation): "A Declaration of the Independence of Cyberspace":

Governos do Mundo Industrial, seus gigantes cansados de carne e aço, eu venho do Ciberespaço, a nova casa da Mente. Em nome do futuro, peço-vos, em nome do passado, que nos deixem em paz. Não sois bem-vindos entre nós. Não tendes soberania onde nos reunimos.

Não temos governo eleito, nem é provável que o tenhamos, por isso dirijo-me a si sem maior autoridade do que aquela com que a própria liberdade sempre fala. Declaro que o espaço social global que estamos a construir é naturalmente independente das tiranias que procura impor-nos. Não têm o direito moral de nos governar nem possuem quaisquer métodos de imposição que tenhamos verdadeiros motivos para temer.

Os governos derivam os seus justos poderes do consentimento dos governados. Não solicitaram nem receberam os nossos. Não o convidámos. Não nos conhece, nem conhece o nosso mundo. O ciberespaço não se encontra dentro das vossas fronteiras. Não pensem que o podem construir, como se fosse um projecto de construção pública. Não pode. É um acto da natureza e cresce por si mesmo através das nossas acções colectivas.

Não se empenhou na nossa grande conversa, nem criou a riqueza dos nossos mercados. Não conhece a nossa cultura, a nossa ética, ou os códigos não escritos que já proporcionam à nossa sociedade mais ordem do que aquela que poderia ser obtida por qualquer uma das suas imposições.

Afirma que existem problemas entre nós que precisa de resolver. Utiliza esta reivindicação como desculpa para invadir os nossos recintos. Muitos destes problemas não existem. Onde houver conflitos reais, onde houver erros, identificá-los-emos e resolvê-los-emos pelos nossos meios. Estamos a formar o nosso próprio Contrato Social. Esta governação surgirá de acordo com as condições do nosso mundo, não com as vossas. O nosso mundo é diferente.

O ciberespaço consiste em transacções, relações, e no próprio pensamento, agrupados como uma onda permanente na rede das nossas comunicações. O nosso é um mundo que está tanto em todo o lado como em lado nenhum, mas não é onde vivem os corpos.

Estamos a criar um mundo em que todos podem entrar sem privilégios ou preconceitos concedidos por raça, poder económico, força militar, ou estação de nascimento.

Estamos a criar um mundo onde qualquer pessoa, em qualquer lugar, pode expressar as suas crenças, por mais singular que seja, sem medo de ser coagida ao silêncio ou à conformidade.

Os seus conceitos legais de propriedade, expressão, identidade, movimento, e contexto não se aplicam a nós. Todos eles se baseiam na matéria, e não há matéria aqui.

As nossas identidades não têm corpos, pelo que, ao contrário de si, não podemos obter ordem por coerção física. Acreditamos que da ética, do interesse próprio esclarecido, e do bem comum, emergirá a nossa governação. As nossas identidades podem ser distribuídas por muitas das vossas jurisdições. A única lei que todas as nossas culturas constituintes reconheceriam geralmente é a Regra de Ouro. Esperamos ser capazes de construir as nossas soluções particulares com base nisso. Mas não podemos aceitar as soluções que está a tentar impor.

Nos Estados Unidos, criou hoje uma lei, a Lei da Reforma das Telecomunicações, que repudia a sua própria Constituição e insulta os sonhos de Jefferson, Washington, Mill, Madison, DeToqueville, e Brandeis. Estes sonhos devem agora nascer de novo em nós.

Tem medo dos seus próprios filhos, uma vez que são nativos num mundo em que serão sempre imigrantes. Porque os temeis, confiais às vossas burocracias as responsabilidades parentais que sois demasiado cobardes para vos confrontardes. No nosso mundo, todos os sentimentos e expressões da humanidade, desde o degradante ao angélico, são partes de um todo ininterrupto, a conversa global de bits. Não podemos separar o ar que se engasga do ar sobre o qual batem as asas.

Na China, Alemanha, França, Rússia, Singapura, Itália e Estados Unidos, está a tentar afastar o vírus da liberdade erguendo postos de guarda nas fronteiras do Ciberespaço. Estes podem manter o contágio fora durante um pequeno período de tempo, mas não funcionarão num mundo que em breve será coberto por meios de comunicação social que suportam bits.

As suas indústrias de informação, cada vez mais obsoletas, perpetuar-se-iam propondo leis, na América e noutros lugares, que afirmam possuir o próprio discurso em todo o mundo. Estas leis declarariam as ideias como sendo mais um produto industrial, não mais nobre do que o ferro fundido. No nosso mundo, tudo o que a mente humana possa criar pode ser reproduzido e distribuído infinitamente, sem qualquer custo. A transmissão global do pensamento já não requer que as suas fábricas o realizem.

Estas medidas cada vez mais hostis e coloniais colocam-nos na mesma posição que os anteriores amantes da liberdade e da autodeterminação que tiveram de rejeitar as autoridades de poderes distantes e desinformados. Temos de nos declarar praticamente imunes à vossa soberania, mesmo que continuemos a consentir o vosso domínio sobre os nossos corpos. Espalhar-nos-emos pelo Planeta para que ninguém possa prender os nossos pensamentos.

Vamos criar uma civilização da Mente no Ciberespaço. Que seja mais humana e justa do que o mundo que os vossos governos fizeram antes.

Davos, Suíça
8 de Fevereiro de 1996[6]

Mesmo quase vinte anos após a publicação desta declaração, o seu texto permanece indiscutivelmente relevante. A sociedade actual está a tentar responder à enorme expansão das tecnologias da informação e da comunicação, ao seu entrelaçamento e interligação, à emergência de novas tendências, etc. No entanto, esta reacção baseia-se muitas vezes principalmente na aplicação e restrição, em vez de compreender e educar os utilizadores.

O ciberespaço, em contraste com o mundo real, é muito específico, e é certamente errado assumir que as mesmas regras funcionarão nele como "offline". Em geral, pode afirmar-se que podem ser aplicados critérios padrão ao ciberespaço, e estes são válidos em relação à localização física real dos dados ou informações. A segunda possibilidade é a criação de novos critérios para a aplicação do princípio de jurisdição local. (Esta é uma localização virtual das relações jurídicas).[7]

É característico do ciberespaço que uma grande parte da sociedade esteja ligada a ele (o envolvimento estimado de cerca de 3,6 mil milhões de pessoas de uma população global de cerca de 7,4 mil milhões de pessoas).[8] Ao mesmo tempo, deve ser declarado que o envolvimento maciço da sociedade começou apenas há cerca de 15-20 anos.

As características do ciberespaço incluem a sua descentralização, globalidade, abertura, riqueza de informação (incluindo informação sob a forma de "smog de informação", completo disparate, meias

---

[6] BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit.23/09/2014]. Disponível em: https://www.eff.org/cyberspace-independence.

[7] Para mais detalhes ver REED, Chris. *Direito da Internet*. Cambridge: Imprensa da Universidade de Cambridge, 2004, p. 218

[8] Ver, por exemplo, *World Internet Users and 2015 Population Stats.* [em linha]. [cit.09/08/2015]. Disponível em: http://www.internetworldstats.com/stats.htm

verdades e mentiras), interactividade e a capacidade de influenciar opiniões através dos utilizadores (avatares[9]). O carácter essencial do ciberespaço é que a tecnologia e serviços relacionados desempenham um papel primordial no mesmo. Recentemente, tornou-se cada vez mais claro que a manifestação do mundo virtual pode ter e tem implicações no mundo real.

A rapidez e especialmente a disponibilidade dos dados transmitidos está a tornar-se um elemento chave da actualidade. Como regra, os utilizadores não querem ou não tentam descobrir onde e como são transmitidos os dados que introduziram nas redes de informação. Também não estão interessados em saber onde se encontra o destinatário dos dados transmitidos ou onde os dados são retidos, pelo que o conteúdo é desmaterializado a partir da estrutura física das redes de informação.

Por um lado, é possível observar uma situação **em que as relações sociais são deslocalizadas no ciberespaço**[10] , o que implica problemas em termos de aplicação da lei, mas por outro lado, esta deslocalização permite aos utilizadores comunicar, enviar, armazenar e alterar dados livremente (e sem restrições sob a forma de fronteiras).

As características do ciberespaço incluem a sua **descentralização, globalidade, abertura, riqueza de informação, interactividade** e a capacidade de influenciar opiniões através de um utilizador. Um atributo essencial do ciberespaço é que a tecnologia e serviços relacionados desempenham um papel primordial no mesmo. Recentemente, tornou-se cada vez mais claro que a manifestação do mundo virtual pode ter e tem implicações no mundo real.

Quanto a uma definição legal de ciberespaço, é possível utilizar, por exemplo, a redacção da Secção 2 (a) da Lei n.º 181/2014 Coll., sobre Cibersegurança[11] , onde se afirma que "*o ciberespaço é um ambiente digital que permite a criação, processamento e troca de informação, consistindo em sistemas de informação, e serviços e redes de comunicações electrónicas"*.

Na nossa opinião, uma das definições mais eficazes de ciberespaço está em Operações de Ciberespaço: Concept Capability Plan 2016-2028, que define o **ciberespaço como um espaço composto por três camadas:** [12]

1. **físico,**
2. **lógico** e
3. **social**.

Estas camadas são então constituídas por um total de cinco componentes.

Anúncio 1) Camada física

Esta camada inclui o termo "**componente geográfica**" e o termo **componentes físicos de rede.** O termo "componente geográfico" significa a localização exacta dos elementos da rede no mundo físico. O termo componentes físicos da rede inclui a infra-estrutura sob a forma de cabos, elementos de controlo da rede (switch, router) e outros dispositivos.

[9] Uso o termo avatar aqui intencionalmente porque é uma expressão de uma identidade virtual criada por um indivíduo real.
O termo avatar vem originalmente do hinduísmo, onde o termo se referia à encarnação de Deus ou da alma libertada em forma corporal na terra (a encarnação terrena de um ser espiritual).
Actualmente, este termo é utilizado como representação visual (ícone ou personagem) de um utilizador no mundo virtual (num jogo, blogue, fórum, Internet, etc.), ou seja, no ciberespaço.

[10] *Delokalizace právních vztahů na internetu* [online]. [cit.15/04/2012]. Disponível em: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

[11] A seguir referida como CSA

[12] TRADOC. Operações de Ciberespaço: Plano de Capacidade do Conceito 2016-2028. [em linha]. [cit. 18/02/2018], pp. 8-9 Disponível em: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

Esta divisão da camada física tem a sua própria lógica. Embora as fronteiras geopolíticas entre Estados possam ser facilmente atravessadas no ciberespaço, no mundo real ainda existem limitações que derivam da natureza do nosso mundo físico.

Traduzir esta ideia num mundo de ataques e incidentes cibernéticos significa que, como atacante, posso danificar um elemento da camada física ou remotamente, por exemplo, conhecendo a sua vulnerabilidade específica que pode ser atacada remotamente, ou posso danificá-lo directamente no mundo real se conseguir chegar a ele fisicamente e atacá-lo, por exemplo, usando a força física. O impacto no ciberespaço será o mesmo, mas a execução do ataque em si é bastante diferente.

Anúncio 2) Camada lógica

Esta camada contém **componentes lógicos de rede**, o que significa ligações lógicas entre nós de rede. Estes são implementados através de protocolos de comunicação em rede. Os nós podem ser computadores, telefones e outros dispositivos de rede.

Anúncio 3) Camada **social**

Esta camada é constituída por componentes chamados **"personalidade cibernética"** e **personalidade**.

A componente "ciberpersonalidade" inclui a identificação de uma pessoa na rede, tais como endereço de correio electrónico, endereço IP, número de telefone e muito mais. A componente "personalidade" consiste em pessoas reais ligadas à rede. Um indivíduo pode então ter múltiplas "personalidades cibernéticas", tais como diferentes e-mails em diferentes dispositivos, e uma "personalidade cibernética" pode na realidade ser várias pessoas reais diferentes, utilizando, por exemplo, uma única conta partilhada.

O ciberespaço também pode ser definido de acordo com a disponibilidade e rastreabilidade dos dados para um utilizador médio. De acordo com esta divisão, o ciberespaço pode ser dividido em serviços e dados disponíveis através da Internet, serviços e dados disponíveis apenas em redes e dispositivos específicos, e serviços e dados intencionalmente escondidos e acessíveis utilizando ferramentas especiais.

Tipicamente, são utilizados os seguintes nomes para estas categorias:

1. **Web de Superfície,**
2. **Deep Web** e
3. **Teia Escura**.

As Teias Profundas e Escuras são também colectivamente referidas como **D4rkN3ts - Darknets.** Todos estes componentes juntos criam o verdadeiro ciberespaço.[13]

Infelizmente, a terminologia onde o termo *teia* é utilizado para dividir o ciberespaço foi influenciada pelo facto de a seguinte equação simples ser válida para a maioria do público em geral:

CIBERESPAÇO = INTERNET = **WEB**

No entanto, o ciberespaço não se refere apenas aos sítios Web, mas a todos os sistemas informáticos, serviços, utilizadores e dados deste espaço.

---

[13] Cf. Por exemplo, *a teia escura explicada.* [online]. [cit. 20/07/2016]. Disponível em: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
ou
Surface Web, Deep Web, Dark Web - What's the Difference. [em linha]. [cit. 20/07/2016]. Disponível em: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

2.2 Âmbito de aplicação da lei no Ciberespaço

O ciberespaço é aberto e facilmente acessível a todos, ***"... não existem leis especiais, e é necessário seguir normas geralmente vinculativas"*** [14]

O facto indiscutível é que a implementação de um número cada vez maior de relações sociais, bem como económicas, está a deslocar-se para o ambiente das redes de informação. Assim, surge a necessidade de uma certa regulamentação legal de tal conduta. Devido à deslocalização de entidades jurídicas em diferentes países em todo o mundo, a questão é qual o sistema jurídico (se houver) que se aplicará a quaisquer actos (ou delitos) cometidos na Internet.

É portanto necessário abordar principalmente duas questões. Em primeiro lugar, se a lei se aplica na Internet e, em caso afirmativo, que normas jurídicas se aplicam. Em segundo lugar, como este direito pode ser exercido, incluindo possíveis sanções ou outras medidas. Um exemplo de aplicação difícil da lei é um caso em 2005, quando um jogador de um jogo online "*The Legend of Mir 3*" **matou outro jogador** na China **por ter roubado uma arma virtual**. Existe um comércio de mercadorias virtuais entre os jogadores deste jogo, bem como um sistema de empréstimo. Isto é especialmente evidente quando alguns jogadores são amigos, mas não é uma condição que eles se conheçam do mundo real. Foi um empréstimo que causou o assassinato. Um jogador chamado Qui Chengwei emprestou um sabre virtual, o "*Sabre do Dragão*", ao seu amigo virtual Zhu Caoyuan. Contudo, Zhu sucumbiu à sedução do dinheiro fácil e vendeu a arma por 7.200 yuan (que é cerca de 19.000-20.000 CZK) num leilão online. Depois de saber da venda, Qui recorreu à polícia e denunciou o roubo do sabre virtual. A polícia recusou-se a tratar do caso, declarando que a propriedade virtual (de artigos essencialmente inexistentes) não está coberta por lei. Qui perdeu a paciência, atacou Zhu em sua casa e esfaqueou-o até à morte.[15]

É óbvio que este é um caso muito extremo, mas demonstra adequadamente que o mundo virtual não está desligado do mundo real. Por conseguinte, a questão da responsabilidade legal no mesmo deve ser abordada.[16] De facto, desde o início do desenvolvimento da Internet, tem existido um conflito entre o mundo técnico e o mundo jurídico. De uma perspectiva técnica, a Internet é logicamente concebida com uma hierarquia e estrutura claras. No entanto, a lei, especialmente a lei local, tem frequentemente injectado "caos" nesta lógica. O termo "caos" talvez descreva muito apropriadamente os esforços da legislação para regular este mundo puramente técnico porque, no ciberespaço, um utilizador tem uma vasta gama de opções para "contornar" uma certa proibição ou restrição. Nos exemplos seguintes, vou tentar demonstrar a interacção do mundo real e virtual.

LICRA vs. Yahoo

Um dos primeiros casos relacionados com a aplicabilidade da lei na Internet ocorreu em França em 2000. Em Fevereiro de 2000, Marc Knobel (um judeu francês que dedicou a sua vida à luta contra o nazismo) visitou o site de leilões www.yahoo.com e descobriu que o servidor oferecia uma série de artigos relacionados com o nazismo ou relacionados com as forças armadas alemãs da Segunda Guerra Mundial nos seus websites. Após esta descoberta, Marc Knobel dirigiu-se ao Yahoo! Inc. solicitando o bloqueio deste site. Yahoo! Inc., no entanto, não acatou o seu pedido. Em 11 de Abril de 2000, Marc Knobel, através da LICRA (Ligue Internationale Contre Le Racisme et l'Antisémitisme) intentou uma acção contra o Yahoo! Inc. num tribunal francês por violação da lei francesa, uma vez que a promoção

---

[14] SMEJKAL, Vladimír. *Internet a §§§*. 2ª actualização. e ext. ed. Praga: Grada, 2001, p. 32

[15] Cf. HAINES, Lester. *Jogador online apunhalado por palavras cibernéticas "roubadas"*. [online]. [cit.03/10/2006]. Disponível em: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

[16] Cf. Decisão do Supremo Tribunal 4 Tz 265/2000, a partir de 16/01/2001. [em linha]. [cit.13/03/2008]. Disponível a partir de: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

e apoio do nazismo na televisão, na rádio e na escrita é proibida em França. Yahoo! Inc. defendeu-se alegando que os servidores em que o portal de leilões opera estão fisicamente localizados nos Estados Unidos, pelo que a lei francesa não pode ser aplicada ao hardware e websites operados nos Estados Unidos. A defesa argumentou ainda que o conteúdo dos sítios web é principalmente destinado a residentes nos EUA, aos quais a Primeira Emenda garante a liberdade de expressão. Qualquer tentativa de remover este website seria então inconsistente com esta Emenda.

No entanto, LICRA salientou que, se o Yahoo! Inc. faz negócios em França, tem de respeitar as leis de França, e a Internet não é excepção. O Yahoo! Inc. respondeu a este argumento que não é capaz de determinar onde os seus clientes estão a entrar no portal do leilão. Por conseguinte, se eliminassem os sites em questão, não só não respeitariam a Primeira Emenda, como impediriam o acesso de todos os utilizadores, independentemente das fronteiras. Isto tornaria a lei francesa de facto lei global. Em 22 de Maio de 2000, o Juiz Jean-Jacques Gomez ordenou à empresa que bloqueasse o acesso dos utilizadores franceses aos sítios Web de leilões dos EUA com memoriais nazis. Ele justificou a sua decisão, inter alia, dizendo que a Yahoo! Inc. pode identificar tão bem os utilizadores franceses que estes podem colocar anúncios em francês nos sítios web que visitam. O juiz deu à Yahoo! Inc. 90 dias para instalar um sistema de filtragem baseado em palavras-chave no Yahoo! Inc. websites franceses. *"O juiz Gomez declarou no raciocínio que é possível bloquear até noventa por cento dos utilizadores franceses de acederem aos sítios web em questão. A solução técnica que o Yahoo! tem de encontrar com base no acórdão será avaliada por um painel internacional de três membros. A sua conclusão anterior afirma que até 70 por cento dos utilizadores podem ser desbloqueados pela designação do seu Fornecedor de Serviços Internet (ISP) e outros 20 por cento através do seguimento de palavras-chave de motores de busca no Yahoo!*" [17]

Greg Wrenn, advogado da Yahoo! Inc., disse: "*Sempre que a palavra Hitler for mencionada numa página comemorativa das vítimas do Holocausto, a página será fechada automaticamente. Não é de todo possível falar de um julgamento eficaz porque, de facto, não é possível cumpri-lo".*

Os problemas técnicos nessa altura eram, e ainda são até hoje, na medida em que apenas aquilo que pode ser claramente definido pode ser filtrado (palavras como Nazi, Heil Hitler, etc.). Mas o filtro não é capaz de detectar todas as versões possíveis de material não desejado (por exemplo, N_A_Z_I, H3Il HiT_L3R, etc.). Estas diferenças podem ser reconhecidas por pessoas singulares (por exemplo, empregados de um determinado ISP), que depois apagam a página; contudo, um operador de um fórum ou leilão repreensível pode simplesmente alterar o endereço e continuar as suas actividades.

Yahoo! Inc. renunciou ao seu recurso contra a sentença do tribunal francês e começou a bloquear os utilizadores franceses de websites que oferecem conteúdos censuráveis. No entanto, a Yahoo! Inc. também solicitou ao tribunal[18] com jurisdição local nos Estados Unidos uma decisão declaratória que excluiria a jurisdição do tribunal francês sobre a empresa americana. Esse tribunal defendeu a opinião da Yahoo! Inc. de que a aplicação da decisão francesa nos Estados Unidos era inconstitucional. A LICRA recorreu dessa sentença. O Tribunal de Recurso dos EUA respondeu negando a sua jurisdição sobre as organizações LICRA. Em 2006, o caso foi para o Supremo Tribunal dos EUA[19] , que se recusou a considerar o caso no final. Assim, as decisões do tribunal dos EUA foram mais favoráveis ao Yahoo! Inc., que se recusou a analisar o caso no final. No entanto, acabou por decidir, voluntariamente, remover completamente os sítios web que ofereciam artigos de temática nazi dos seus servidores, não apenas em França.

Gutnick vs. Dow Jones

[17] ŠTOČEK, Milão. V *Hitlerově duchu proti Hitlerovi.* [online]. [cit.10/07/2016]. Disponível em: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

[18] Tribunal Distrital dos Estados Unidos para o Distrito do Norte da Califórnia em San Jose

[19] Supremo Tribunal dos Estados Unidos

Joseph Gutnick (um empresário de diamantes australiano) leu um artigo sobre si próprio numa edição online do jornal *Barron's*[20] em 2000, que ele considerou difamatório. Gutnick entrou com um processo por difamação contra a Dow Jones num tribunal australiano. A Dow Jones utilizou argumentos semelhantes aos do Yahoo! Inc. na sua disputa com o LICRA. O argumento baseou-se principalmente no facto de a versão impressa do jornal se destinar principalmente ao mercado dos EUA, pelo que o caso não pode ser abrangido pela lei australiana.

Apesar deste argumento, o tribunal australiano decidiu[21] em 2002[22] da seguinte forma: *"Uma vez que o material (artigo) também está disponível na Austrália, o local onde Gutnick é mais conhecido, a difamação pode fazer-lhe o maior mal. A Dow Jones é obrigada a pagar uma indemnização a Gutnick".* O tribunal disse que não iria considerar se a Internet tem ou não limites, tendo em conta em particular onde o conteúdo estava disponível, e não onde foi publicado. O tribunal declarou também que todos têm direito a protecção legal contra conduta semelhante ou outros ataques. Na sua sentença, o tribunal australiano também notou a realidade da natureza transfronteiriça da Internet, o que corresponde ao extenso exercício da jurisdição.

GoDaddy

GoDaddy[23] é o registador maioritário de domínios de Internet dos EUA. Em 2016, gere mais de 61 milhões de domínios da Internet, fazendo da GoDaddy o maior registador de domínios. Registar um domínio junto deste ISP é muito simples e acessível. Ao mesmo tempo, devido à localização da empresa nos EUA, os utilizadores recebem protecção legal para os seus dados pessoais e dados listados num domínio registado sob o GoDaddy, desde que os utilizadores não violem a lei dos EUA. Por esta razão, os domínios registados com GoDaddy são muito frequentemente utilizados, por exemplo, por grupos extremistas, racistas e outros grupos ou utilizadores. Estes utilizadores dependem então da lei constitucional dos EUA e da Primeira Emenda à Constituição dos EUA:

"O Congresso não fará qualquer lei que respeite um estabelecimento religioso, ou que proíba o seu livre exercício; ou que abranja a liberdade de expressão, ou de imprensa; ou o direito do povo a reunir-se pacificamente, e a solicitar ao governo uma reparação das queixas".[24]

O problema ao abordar o crime cibernético com o conteúdo acima referido é provar a realidade da ameaça ou do crime para que não constitua uma violação da Primeira Emenda à Constituição.

Second Life (e pornografia "infantil").

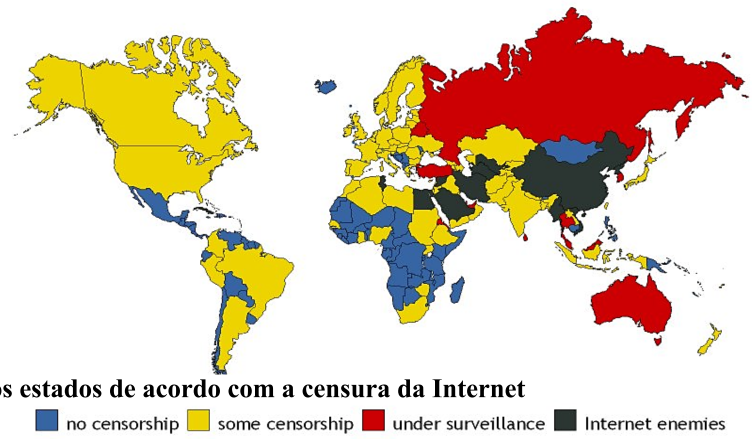
Second Life é um ambiente virtual 3D desenvolvido pela Linden Lab. Este ambiente permite-lhe criar os seus próprios avatares e utilizá-los para interagir com outros, com a possibilidade de gerar lucro. Second Life está dividido em dois mundos virtuais, de acordo com a idade de um utilizador.[25] Os utilizadores podem alterar a sua identidade e modificar a aparência do avatar de acordo com as suas ideias. Em 2007, a estação alemã ARD e posteriormente a CNN chamou a atenção para a existência de uma "ilha pedófila".[26]

Este relatório aponta para o facto de alguns utilizadores MainGrid (ou seja, utilizadores com mais de 18 anos) terem criado avatares sob a forma de uma criança e outros fingiam ser adultos. Como parte

---

[20] http://online.barrons.com
[21] Tribunal Superior da Austrália
[22] Acórdão [2002] HCA 56 em 10 de Dezembro de 2002, [online]. [cit.24/03/2014]. Disponível a partir de: http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html
[23] https://uk.godaddy.com/
[24] *Primeira Emenda.* [em linha]. [cit.10/07/2016]. Disponível a partir de: https://www.law.cornell.edu/constitution/first_amendment Tradução do autor
[25] **MainGrid** - destinado a utilizadores a partir dos 18 anos; **TeenGrid** - destinado ao grupo etário dos 13 aos 18 anos.
[26] Para mais pormenores, ver: *CNN sobre sexo pedófilo no Second Life.* [online]. [cit.18/06/2009]. Disponível em: http://www.youtube.com/watch?v=AQM-SiiaipE

da interacção mútua, os avatares de crianças foram abusados por avatares adultos. As autoridades responsáveis pela aplicação da lei na Alemanha lançaram uma investigação porque a posse de pornografia infantil virtual é um crime ao abrigo do direito penal alemão.[27] A Linden Lab cooperou com as autoridades alemãs na identificação dos utilizadores e proprietários das parcelas virtuais em que a pornografia infantil virtual teve lugar. Na República Federal da Alemanha e no Reino Unido, a conduta em questão era punível pelo direito penal, mas nos Estados Unidos tal conduta não era passível de procedimento criminal.



Divisão dos estados de acordo com a censura da Internet

Actualmente, não há nenhum Estado no mundo que renuncie ao direito de punir uma infracção que afecte os interesses que protege.

Para além dos casos acima referidos, há uma série de outros exemplos de regulamentação da Internet e de serviços da Internet prestados por organizações ou Estados. Este regulamento implica então necessariamente problemas com a aplicabilidade e execução da lei.

O mapa apresentado[28] mostra que a maioria dos países do mundo adoptou instrumentos legais que afectam a Internet ou os serviços prestados.

Do ponto de vista de um utilizador, deve ser afirmado que o princípio da territorialidade em ligação com a Internet perde o seu significado porque pode ser localizado em qualquer parte do mundo a qualquer momento, sem que um utilizador tenha de saber onde se encontra o servidor com o qual está a comunicar. Deste ponto de vista, a Internet é global e não conhece fronteiras.

"É verdade que uma localização física de determinada informação pode ser rastreada em qualquer altura - mas a localização é frequentemente aleatória, de muito curto prazo e geralmente completamente irrelevante para a informação enquanto tal e para os seus efeitos legais".[29]

A lei deve acompanhar o ritmo do mundo virtual, mas infelizmente isto nem sempre funciona como estados (fechados em territórios fixos) muitas vezes não dispõem dos meios para fazer cumprir efectivamente a lei dentro do ciberespaço.[30] Basicamente, há duas maneiras de abordar este problema.

---

[27] *Alegação de 'abuso de crianças' no Second Life.* [em linha]. [cit. 16/06/2009]. Disponível a partir de: http://news.bbc.co.uk/2/hi/technology/6638331.stm

[28] *Censura da Internet.* [em linha]. [cit.10/08/2016]. Disponível em: http://www.deliveringdata.com/2010_10_01_archive.html

[29] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 7

[30] Cf. declarações no âmbito da **Declaração da Independência do Ciberespaço**.
Cf. THOMAS, Douglas. *A criminalidade na Fronteira Electrónica.* Em Cibercriminalidade. Em Londres: Routledge, 2003, p. 17 e seguintes.
Cf. JOHNSON, David R. e David POST. *A Ascensão da Lei no Ciberespaço.* [online]. [cit.10/07/2016]. Available from: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013

Uma possibilidade é respeitar os princípios de territorialidade dos Estados tal como são hoje estabelecidos. Esta abordagem significaria então essencialmente que, se alguém interferisse com os direitos que o Estado garantiu proteger, teria de esperar até o agressor estar na jurisdição física do Estado[31] , ou o agressor teria de recorrer à assistência jurídica internacional.

A segunda opção é criar legislação especial, a chamada jurisdição da Internet, que se aplicaria ao mundo online. A questão é como este novo direito seria adoptado pelos países individualmente. Pessoalmente, acredito que, nas condições actuais, não é possível unir todos os ramos do direito a nível mundial (civil, comercial, criminal, administrativo, etc.), nos quais a Internet intervém de alguma forma. Baseio a minha afirmação no facto de que a Convenção sobre o Cibercrime, que define os grupos básicos de crimes que devem ser processados no ciberespaço, foi adoptada em 2001, mas a partir de 1 de Agosto de 2016, apenas 49 países a tinham ratificado.

Dada a natureza global da Internet, também parece ser problemático **determinar:**

1. **lei aplicável** (ao abrigo da qual a lei do Estado o potencial litígio será decidido),
2. **autoridade competente para emitir uma decisão**,
3. **Autoridade que pode impor ou executar directamente uma decisão**.[32]

Para além das normas jurídicas clássicas, as *autoridades definidoras* participam na criação da lei ou regras na Internet através da criação de *normas definidoras.*

07111700811500702511711210101306112105603611908411808902808506704302300105809312007008406908508901200001912712009107811509012501712003001400010109503110900309406906911131141121 02&EXT=pdf

[31] Um exemplo desta abordagem pode ser o caso em que um utilizador da República Checa, por exemplo, atacará pública e repetidamente um país na Internet (por exemplo, por incumprimento dos direitos humanos no referido país, etc.), ou realizará outras actividades ilegais no país visado (embora não seja ilegal na República Checa). Se um tal utilizador decidir, a qualquer momento no futuro, visitar o país contra o qual agiu, a lei territorial do país pode ser-lhe aplicada ao atravessar as fronteiras para esse país.

[32] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 7

RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

- Para compreender as questões de leis e regulamentos que regem a ciber-segurança, são necessários pelo menos os princípios básicos do funcionamento do direito, a sua divisão e implementação. Os dois primeiros capítulos apresentam o quadro geral da aplicabilidade da lei no ciberespaço.
- Uma norma legal representa uma regra de conduta geralmente vinculativa que regula os direitos e obrigações das entidades. Esta norma de conduta é expressa numa forma jurídica especial reconhecida pelo Estado (ou pela União Europeia), e a sua observância é assegurada pela execução estatal.
- A lei é uma das suas possíveis regulamentações sob a forma de construções normativas imperfeitas, onde se aplica mais do que em qualquer outro lugar que entre a conduta na realidade, ou seja, o que é realmente realizado no ambiente da Internet, e a conduta normativa, ou seja, o que deveria ser (pela vontade do regulador e a nossa), não se equipara. A realidade da Internet e os seus regulamentos normativos são, portanto, duas categorias relativamente separadas. Este pressuposto também não será posto em causa nesta publicação. Pelo contrário, será um dos seus pilares.
- O ciberespaço é:
  - um espaço de actividades cibernéticas, ou um espaço criado pelas tecnologias de informação e comunicação onde é criado um mundo virtual (ou espaço) paralelo ao espaço real.
  - um ambiente digital que permita a criação, processamento e troca de informação, constituído por sistemas de informação, e serviços e redes de comunicações electrónicas.
  - um espaço composto por três camadas: física, lógica e social.
- Exemplos da aplicação da lei no ciberespaço foram apresentados em estudos de casos individuais.

PALAVRAS-CHAVE A LEMBRAR

- lei
- norma legal
- ciberespaço

PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- O que é a lei?

- O que é uma norma legal, e como está dividida?
- O que é o ciberespaço?
- Em que camadas consiste o ciberespaço?
- A lei aplica-se no ciberespaço e, em caso afirmativo, que normas legais se aplicam?
- Como pode a lei ser aplicada no ciberespaço, incluindo possíveis sanções ou outras medidas?
- Dar alguns exemplos da aplicação da lei no ciberespaço.

3. Base jurídica da actividade do ISP (Internet service provider)

As autoridades definidoras participam na criação da lei na Internet, na restrição ou expansão das suas actividades, através da criação de *normas definidoras. A* fim de compreender a questão de uma eventual responsabilidade dos prestadores de serviços da sociedade da informação, tenho primeiro de caracterizar as normas definidoras e a autoridade que as define.

A definição de normas é criada e implementada por entidades autorizadas a definir o ambiente da rede de informação. Na prática, estas são normas *sui generis* que definem redes de informação como tal. Ocorrem em camadas que são interdependentes. *"A definição de normas é criada por operadores de telecomunicações, produtores de software de escritório mas também, por exemplo, criadores ou operadores de jogos em linha, ou qualquer pessoa que abra um blogue ou tenha uma caixa de correio electrónico. (Uma norma definidora criada por um utilizador desta caixa é um filtro que realiza automaticamente uma operação de caixa de entrada definida)".* [33]

As autoridades definidoras são os criadores das normas definidas. É uma entidade que, através do seu funcionamento, cria regras para o funcionamento do sistema lógico em que a autoridade opera. Como mencionado anteriormente, a ICANN tem uma posição executiva entre estas autoridades, uma vez que é responsável pela atribuição, administração e estabelecimento de regras para o sistema de nomes de domínio.[34] Outra autoridade definidora é, por exemplo, a IETF.[35] Embora as autoridades definidoras possam parecer ser administradores ilimitados do ciberespaço, continuam a estar sujeitas à lei de um Estado. [36]

A especificidade da **Internet** é que ela **só existe graças à definição das autoridades**. **É composta por elas. Nenhuma operação terá lugar sem a participação** (execução ou mediação da operação) **da autoridade que a define**.

Lawrence Lessig afirma no seu livro Código e Outras Leis do Ciberespaço (Código v. 2): "*Podemos construir, desenhar ou codificar*[37] *(programar) ciberespaço para proteger os valores que consideramos fundamentais. Mas também podemos desenhá-lo ou programá-lo, deixando desaparecer estes valores. Não há meio-termo, tudo no ciberespaço é construído de alguma forma. Nunca descobrimos o código, criamo-lo sempre"*.[38]

Seguindo a afirmação acima e a minha experiência com o ciberespaço, atrevo-me a dizer que a maior **autoridade definidora**, mesmo que não seja a entidade que cria as regras de funcionamento do

---

[33] Cf. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 42 e seg., p. 88 e seg., p. 88 e seg.
O RFC (*Request For Comments*) também pode ser incluído nas normas de definição. Embora estes sejam documentos com a natureza de recomendações e não de normas, são respeitados pelos utilizadores como se fossem normas. Os RFCs estão disponíveis gratuitamente em http://www.ietf.org/rfc.html.
[34] O nome de domínio é utilizado para denotar a "classe" dos sistemas informáticos ligados à Internet. Caracterizam-se por uma certa unidade geográfica e organizacional: por exemplo, todos os computadores no domínio **. cz** estão localizados na República Checa. Todos os computadores do domínio (subdomínio) **nic.cz** são computadores sob a administração da associação CZ.NIC. Os nomes dos domínios principais (com base na geografia) estão estritamente separados.
Relativamente aos nomes de domínio, Polčák afirma, entre outras coisas, que: "Uma forma de **realidade virtual** pode ser um nome de domínio. É um registo nas bases de dados DNS. **Se a autoridade de domínio decidir eliminar o nome de domínio, esta realidade virtual deixará de existir.** Não importa se se trata de um nome de domínio como: www.tondovy_stranky.cz ou www.google.com.
[35] IETF - The Internet Engineering Task Force. Para mais detalhes, ver https://www.ietf.org/.
[36] É sempre uma pessoa singular ou colectiva que tem a sua sede social ou residência permanente. Por conseguinte, estão sujeitas à lei como qualquer outra entidade. Em alguns países (por exemplo, **a China**), a autoridade que define a lei é o próprio Estado.
[37] Lessig refere-se à **norma definidora** como **código**.
[38] Cf. LESSIG, Lawrence. *Código v. 2. p.* 6 Disponível na íntegra (Eng) [online]. [cit.13/03/2008]. Disponível a partir de: http://pdf.codev2.cc/Lessig-Codev2.pdf

sistema lógico, **é um utilizador enquanto tal**. A sua função definidora actua indirectamente. Um utilizador de serviços prestados por cada FSI influencia directa ou indirectamente o que será bem sucedido no ciberespaço e o que não o será. Se um grupo suficientemente grande de utilizadores decidir deixar de utilizar activamente qualquer dos serviços prestados por um ISP, esse serviço será forçado a alterar a sua "conduta" com base na procura dos utilizadores, ou, na pior das hipóteses, deixará de existir. É uma questão de quão grande grupo de pessoas teria de deixar de utilizar serviços como o Google, Microsoft, Facebook, etc., para que não seja marginal para estas empresas. No entanto, é o ciberespaço onde os utilizadores têm a oportunidade de influenciar directamente o funcionamento ou não funcionamento de serviços individuais.

Por conseguinte, podem ser tiradas as seguintes conclusões:

- **O ciberespaço é formado pela vontade de definir autoridades.**
- **Todos os prestadores de serviços da sociedade da informação estão a definir autoridades.**
- **Todos os prestadores de serviços, como qualquer outro organismo de direito, são legalmente responsáveis pelas suas acções.**

A questão da responsabilidade dos fornecedores de serviços da sociedade da informação (ISP) ao abrigo da Lei sobre Certos Serviços da Sociedade da Informação é aqui mencionada intencionalmente, uma vez que está directamente relacionada com a questão do cibercrime, a responsabilidade do utilizador, e a descoberta e segurança de informações relevantes para os procedimentos criminais. *"Em geral, o princípio é que se a informação for ilegal e um FSI não tiver conhecimento da sua criação ou comunicação, o FSI está isento de responsabilidade por lei*" [39]

Para além da lei acima referida, o termo prestador de serviços é também definido, por exemplo, na Convenção sobre o Cibercrime, especificamente no artigo 1 (c) onde se afirma que o prestador de serviços é:

- qualquer entidade pública ou privada **que forneça aos utilizadores do seu serviço a capacidade de comunicar por meio de um sistema informático**, e
- qualquer outra entidade **que processe ou armazene dados informáticos em nome de tal serviço de comunicação ou utilizadores de tal serviço.**

3.1 Regulamentação das actividades dos ISP na República Checa

A norma jurídica básica que caracteriza as actividades dos ISP na República Checa é a Lei n.º 480/2004 Coll., sobre certos serviços da sociedade da informação[40] . Esta lei é uma implementação da Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho de 9 de Setembro de 2015 que estabelece um procedimento para a prestação de informações no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação.[41]

A Lei checa sobre certos serviços da sociedade da informação reconhece os seguintes três prestadores de serviços, estipulando que um prestador de serviços é qualquer pessoa singular ou colectiva que preste qualquer um dos serviços da sociedade da informação: [42]

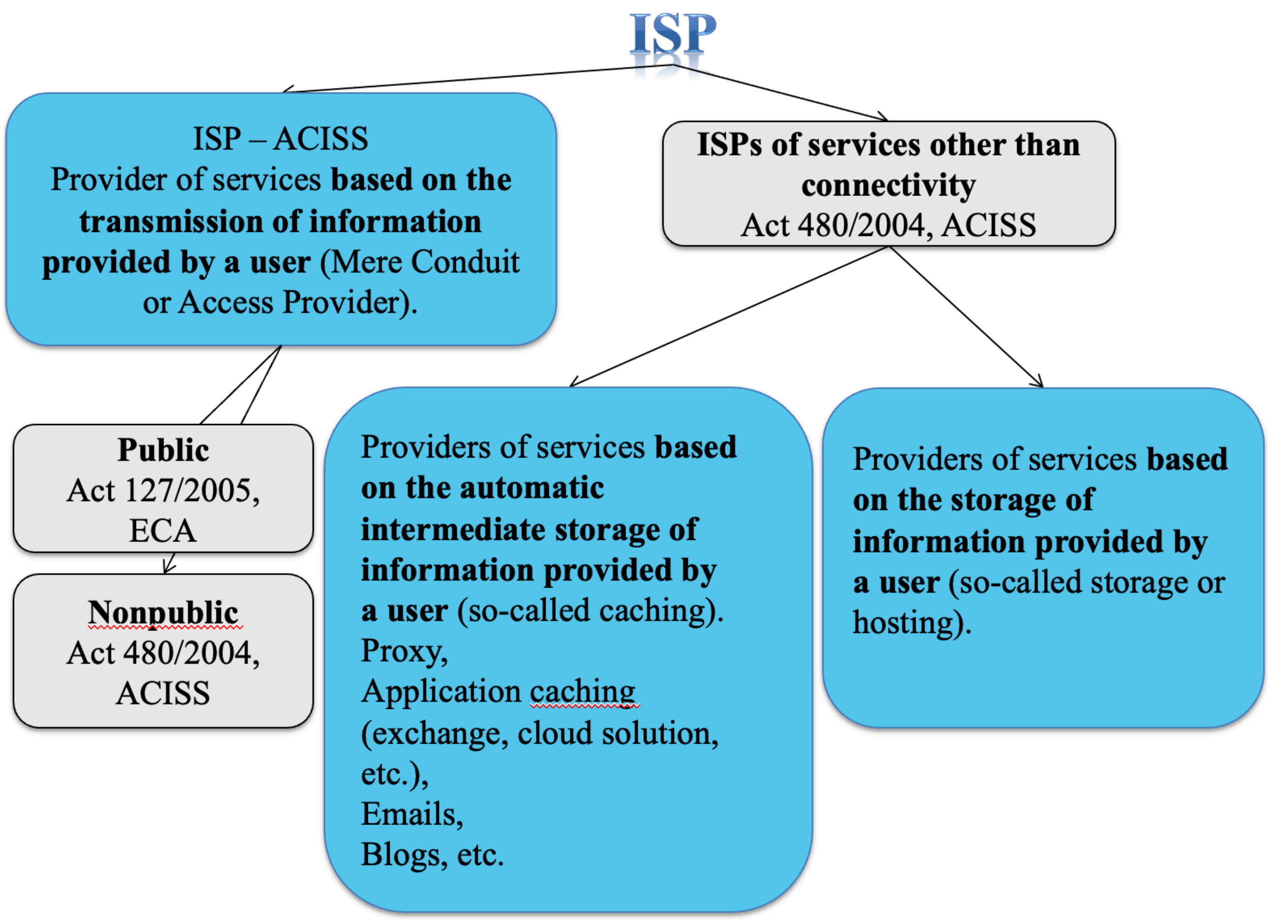
---

[39] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 55
[40] A seguir referida como a lei sobre certos serviços da sociedade da informação ou ACISS
[41] Disponível online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535&qid=1624364501265
[42] Ver Secção 2 (d) do ACISS

1. **Prestadores de serviços baseados na transmissão de informações fornecidas por um utilizador** (Mere Conduit ou Access Provider).
2. **Prestadores de serviços baseados no armazenamento automático intermédio de informações fornecidas por um utilizador** (o chamado caching).
3. **Prestadores de serviços baseados no armazenamento de informação fornecida por um utilizador** (o chamado armazenamento ou hosting).

Nenhuma pessoa é excluída da definição acima. (Não tem de ser, por exemplo, uma pessoa a fazer negócios ao abrigo de outro regulamento legal). No entanto, se outros regulamentos especiais se aplicarem a um fornecedor (ver, por exemplo, um dos fornecedores de ligação), estes devem também segui-los.

Em termos gráficos, é possível mostrar os fornecedores listados (e a vinculação por regulamentos legais individuais) da seguinte forma:



Um destinatário de um serviço da sociedade da informação é um utilizador que pode ser qualquer pessoa singular ou colectiva que utilize o serviço da sociedade da informação, nomeadamente com o objectivo de procurar informação ou torná-la acessível.[43]

De acordo com a Lei sobre Certos Serviços da Sociedade da Informação, **serviço da sociedade da informação** significa *"qualquer serviço prestado por via electrónica a pedido individual de um utilizador apresentado por via electrónica, normalmente prestado mediante remuneração. Um serviço será fornecido por meios electrónicos se for enviado através de uma rede de comunicação*

[43] Ver Secção 2 (e) do ACISS

electrónica e recolhido pelo utilizador a partir de equipamento electrónico para armazenamento de dados" [44]

A definição dada na legislação checa baseia-se então directamente na Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho [Artigo 1(b)], que estabelece que um serviço é *"qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante* ***remuneração, à distância, por via electrónica e a pedido individual de um destinatário de serviços".***

Desta definição decorrem quatro características básicas de um serviço:

- é fornecido por meios electrónicos,
- é fornecido a pedido individual de um utilizador,
- é normalmente fornecido para remuneração,
- é fornecido remotamente (à distância).

O conceito de prestação por **via electrónica está** estabelecido na Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, no artigo 1 (b) (ii), onde é definido como um serviço que é enviado inicialmente e recebido no seu destino através de equipamento electrónico para o processamento (incluindo a compressão digital) e armazenamento de dados. Este serviço é inteiramente transmitido, transportado e recebido por fio, rádio, meios ópticos ou outros meios electromagnéticos. O regulamento checo utiliza uma lista demonstrativa que afirma que se trata principalmente de uma rede de canais electrónicos, equipamento de comunicação electrónica, sistemas automáticos de chamada e comunicação, equipamento terminal de telecomunicações e correio electrónico. [45]

Um **pedido individual de utilizador** significa que deve ser uma actividade activa de um utilizador. Husovec declara que diz respeito a casos em que, por exemplo, um utilizador introduz um endereço no campo do navegador (IE, Firefox, Chrome, etc.), formulando assim um pedido para abrir a página relevante, ou escreve uma mensagem SMS. De acordo com Husovec, um exemplo típico de um serviço que é fornecido sem um pedido individual é, por exemplo, a transmissão televisiva.[46]

O critério mais problemático para definir um serviço da sociedade da informação é o facto de **ser prestado** um **serviço mediante remuneração.** O regulamento checo também copia o regulamento internacional sobre este ponto e contém uma disposição "*normalmente em troca de remuneração*". No ambiente da Internet ou de outras redes informáticas, há uma série de serviços que são prestados "gratuitamente". A Husovec argumenta com toda a razão que, sob o termo remuneração, é possível imaginar uma série de factos diferentes do desempenho puramente monetário.[47] Pode tratar-se de um desempenho que assumirá a forma de não-monetário, em que um ISP obtém informações sobre os utilizadores sob a forma de dados pessoais, técnicos e outros, tempo gasto na utilização do serviço, oferece uma publicidade do utilizador para outros produtos, etc. Contudo, mesmo esta condição deve ser interpretada de forma mais extensiva, de acordo com Husovec, o que significa que é realizada uma actividade *potencialmente económica.*[48]

Devido ao facto de o termo remuneração poder significar possibilidades realmente diferentes (por exemplo, um agradecimento, visita a um sítio ou link, pagamento financeiro ou outro) e devido à redacção da Lei sobre certos serviços da sociedade da informação (ver *"normalmente para*

---

[44] Ver secção 2 (a) do ACISS
[45] Ver Secção 2 (c) do ACISS
[46] Para mais detalhes ver HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praga: CZ.NIC, 2014, p. 100
[47] Ibidem, p. 98.
[48] Ibidem, p. 99.

remuneração"), pode-se concluir que as actividades de um prestador de serviços da sociedade da informação também podem ser fornecidas gratuitamente.

O termo **à distância** é definido pela Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho como um serviço que é prestado sem que as partes estejam simultaneamente presentes.[49]

Na sua monografia, Husovec dá também exemplos que demonstram o que pode ser considerado um serviço da sociedade da informação. De acordo com a Directiva 2000/31/CE do Parlamento Europeu e do Conselho, uma série de actividades que têm lugar no mundo em linha devem ser incluídas neste conceito. Podem ser vendas em linha de bens, serviços que fornecem informação em linha, comunicação comercial, ou serviços que fornecem ferramentas de pesquisa, acesso e recuperação de dados, serviços que fornecem transmissão de informação através de uma rede de comunicação, etc.

"O poder judicial do Tribunal de Justiça da UE já reconheceu directa ou indirectamente, por exemplo, o serviço AdWords (serviço de publicidade no motor de busca Google)[50] *, serviços de seguro automóvel através da Internet*[51] *, vendas on-line de lentes de contacto*[52] *, ligação à Internet*[53] *, reservas de hotel através de e-mail*[54] *, serviços de agências de viagens através de e-mail*[55] *, servidor de leilões eBay*[56] *e pesquisa tradicional no Google".* [57]

3.1.1 Prestadores de serviços baseados na transmissão de informações fornecidas por um utilizador (Mere Conduit ou Access Provider)

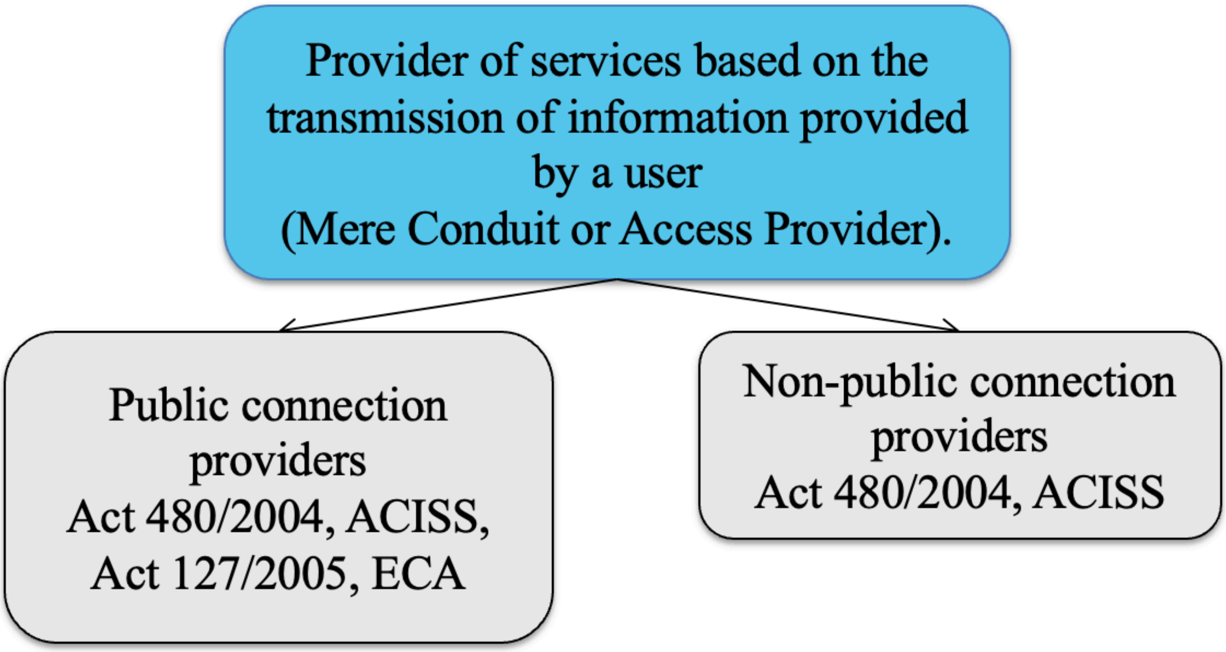
Do ponto de vista da lei sobre certos serviços da sociedade da informação, tal fornecedor pode ser qualquer pessoa singular ou colectiva capaz de fornecer a outras entidades (pessoas singulares ou colectivas) o serviço de transmissão de informação (fornecida pelos utilizadores) através de redes de comunicações electrónicas ou organizando o acesso a redes de comunicações electrónicas para efeitos de transmissão de informação.

Tal fornecedor não será apenas uma pessoa que faz negócios no domínio da ligação de outros a redes informáticas ou à Internet (normalmente serão pessoas registadas no *Registo de Empresários em Comunicações Electrónicas sob a autorização geral*)[58] , mas será qualquer pessoa que forneça ou medique a transmissão de informações através de redes de comunicações electrónicas. É portanto possível imaginar uma situação em que um fornecedor de ligação de acordo com esta lei será uma pessoa que estabelece e disponibiliza a terceiros, por exemplo, ligação Wi-Fi dentro de um restaurante, edifício de apartamentos, casa, etc. Esta categoria incluirá também, por exemplo, escolas (tipicamente universidades que fornecem aos seus estudantes e professores conectividade dentro da sua rede ou à Internet). Contudo, os serviços baseados na transferência de informação incluem também, por exemplo, a aplicação Skype, ICQ, etc. Podemos muito simplesmente descrever estes fornecedores como **fornecedores de ligação.**

---

[49] Ver artigo 1 (b) (i) da presente directiva.
[50] Decisão *Google France* C-236/08 a C-238/08.
[51] Decisão *Bundesverband* C-298/07.
[52] Decisão *Ker-Optika* C-108/09.
[53] Decisão *Promusicae* C-275/06 e *Tele 2*. C-557/07
[54] Decisão *Alpenhof* C-144/09.
[55] Decisão *Pammer* C-585/08.
[56] Decisão *L'Oreal v. Ebay* 324/09.
[57] HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praga: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, pp. 101-102.
[58] A base de dados de empresários em comunicações electrónicas de acordo com a autorização geral está disponível em linha: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

Contudo, a fim de definir os direitos e obrigações individuais dos fornecedores de ligação, estes fornecedores precisam de ser divididos em dois grupos, **públicos e não públicos.** Ambos os grupos de fornecedores de ligação são abrangidos pela Lei sobre certos serviços da sociedade da informação, mas os fornecedores de ligação pública são também abrangidos pela Lei das Comunicações Electrónicas, que estabelece outros direitos e obrigações para estes fornecedores. O *Registo de Empresários de Comunicações Electrónicas* acima mencionado, *de acordo com a autorização geral* administrada pelo Gabinete Checo de Telecomunicações, ajudará a determinar se o fornecedor está incluído em que grupo.



3.1.1.1 Direitos e obrigações do prestador de serviços com base na transmissão de informações fornecidas por um utilizador de acordo com ACISS

A Lei sobre Certos Serviços da Sociedade da Informação no caso de um fornecedor de ligação limita tanto quanto possível a responsabilidade desta entidade pela informação transmitida. No entanto, são estabelecidos requisitos e condições especiais para os operadores de serviços de comunicações electrónicas. Estas condições estão estabelecidas na Lei das Comunicações Electrónicas. As disposições do artigo 12º da Directiva 2000/31/CE permitem que os Estados-membros ordenem a um fornecedor que suspenda a prestação de serviços através dos quais as informações são transmitidas quando os referidos serviços interferem indevidamente com os direitos de outro. Esta opção é um meio de evitar infracções. A ordem de suspensão da prestação de serviços é normalmente emitida por um tribunal.

Um fornecedor de **ligação** só pode **ser responsabilizado pelo conteúdo da informação** se:

- inicia uma tal transmissão,
- selecciona o utilizador da informação transmitida, **ou**
- selecciona ou altera o conteúdo da informação transmitida. [59]

[59] Estas três opções tornam um fornecedor de ligação essencialmente responsável apenas se for uma entidade que envie ou manipule activamente a informação transmitida.

Nos termos da Secção 6 do ACISS, um **fornecedor de ligação não é obrigado** a supervisionar o conteúdo da informação transmitida ou a verificar activamente a ilegalidade da informação transmitida. Um fornecedor não pode ser considerado responsável pela qualidade da informação (que não lhe pode ser atribuída), mesmo que esteja consciente da ilegalidade da informação transmitida.[60]

3.1.1.2 Direitos e obrigações do prestador de serviços com base na transmissão de informações fornecidas por um utilizador de acordo com a Lei n.º 127/2005 Coll.

Os fornecedores de ligações públicas são também regidos pela Lei n.º 127/2005 Coll., sobre Comunicações Electrónicas[61] . Esta lei define alguns termos que utiliza posteriormente. Para os fins desta monografia, estes são em particular:

- **Serviço de comunicações electrónicas** [Secção 2 (n) da ECA[62]]. De acordo com a Secção 2 (n) da ECA, este termo significa um serviço que é normalmente prestado mediante remuneração e baseia-se (total ou principalmente) na transmissão de sinais através de redes de comunicações electrónicas. Este serviço não inclui serviços que ofereçam conteúdos através de redes e serviços de comunicações electrónicas ou que exerçam supervisão editorial sobre conteúdos transmitidos por redes e fornecidos por serviços de comunicações electrónicas. Além disso, este serviço não inclui serviços da sociedade da informação que não se baseiem total ou principalmente na transmissão de sinais através de redes de comunicações electrónicas.
- **Serviço de comunicações electrónicas publicamente disponível** [Secção 2 (o) da ECA]. Este serviço é um serviço de comunicações electrónicas que ninguém está excluído de utilizar previamente.

  A não exclusão significa a possibilidade de celebrar um contrato com uma entidade empresarial que preste um serviço de comunicações electrónicas publicamente disponível. É importante que este serviço esteja aberto a um vasto leque de pessoas, nenhuma das quais está excluída de antemão. O contrário de um tal serviço pode ser, por exemplo, a adesão a várias associações, câmaras, ou, por exemplo, o estatuto de aluno de uma escola.
- **Uma entidade empresarial** que fornece ou está autorizada a fornecer uma rede pública de comunicações ou recursos conexos é referida por este acto como um **operador** [Secção 2 (e) da ECA].
- **Assinante** [Secção 2 (a) da ECA] é qualquer pessoa que celebrou um contrato para o fornecimento de tal serviço com uma entidade empresarial que forneça serviços de comunicações electrónicas publicamente disponíveis. **Utilizador** [Secção 2 letra n) ZoEK] é qualquer pessoa que utilize ou solicite um serviço de comunicações electrónicas publicamente disponível.

A Lei das Comunicações Electrónicas introduziu, com base na Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, *relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Directiva 2002/58/CE*[63] , a obrigação de conservar preventivamente os **dados de tráfego e de localização**[64] sobre comunicações electrónicas. Esta

[60] Cf. artigo 12º da Directiva 2000/31/CE e as disposições da Secção 3 (1), (2) da Lei nº 480/2004 Coll.
[61] A seguir referida como TCE
[62] A seguir referida como TCE
[63] A seguir referida como a **Directiva de Retenção de Dados.** O termo retenção de dados significa o armazenamento generalizado de dados de tráfego e de localização em fornecedores de ligações (na República Checa, em fornecedores ao abrigo da Lei das Comunicações Electrónicas).
[64] Ver Secção 97 (4) da ECA.

obrigação aplica-se apenas a uma entidade empresarial que forneça ou esteja autorizada a fornecer uma rede pública de comunicações ou recursos conexos.

O objectivo da directiva relativa à conservação de dados era **harmonizar as regras dos Estados-Membros sobre a obrigação dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações** de conservarem os dados de tráfego e de localização, para que estes possam ser fornecidos às autoridades competentes dos Estados-Membros para **prevenção, investigação, detecção e repressão de crimes graves, como o terrorismo e a criminalidade organizada.**

O âmbito da directiva foi definido na área dos dados de tráfego e localização sobre pessoas singulares e colectivas e sobre os dados conexos necessários para identificar o assinante ou o utilizador registado.

Esta directiva não se aplicava ao conteúdo das comunicações electrónicas nem às informações necessárias quando se utilizava uma rede de comunicações electrónicas.

Nos termos da directiva, os Estados-membros eram **obrigados a assegurar que os dados de telecomunicações fossem retidos durante um mínimo de seis meses e um máximo de dois anos a partir da data da comunicação**. A directiva foi transposta sob diversas formas para os sistemas jurídicos dos Estados-Membros da UE. No entanto, desde o seu início, houve conflitos de opinião sobre a directiva enquanto tal. Os opositores argumentaram que a directiva interfere de forma desproporcionada com os direitos humanos e liberdades fundamentais, em particular ao exigir essencialmente a recolha generalizada de informações sobre os utilizadores individuais. Foi ainda argumentado que a directiva (numa forma tão geral) não seria capaz de passar no teste de proporcionalidade.

O **teste de proporcionalidade** é um instrumento jurídico padrão tanto dos tribunais internacionais como dos tribunais constitucionais (nacionais) ao avaliar o conflito de disposições da ordem jurídica que procuram proteger um direito ou interesse público constitucionalmente garantido com outro direito ou liberdade fundamental. O teste de proporcionalidade inclui três critérios para avaliar a admissibilidade de uma intervenção:

1. O **princípio da adequação** (adequação ao fim a que se destina), segundo o qual a **medida em questão deve ser capaz de atingir o objectivo pretendido** em geral, que é a protecção de outro direito fundamental ou bem público.
2. O **princípio da necessidade**, que estipula a **utilização apenas dos meios mais amigos do ambiente para atingir o objectivo desejado** (interferência nos direitos e liberdades fundamentais) a **partir de vários meios possíveis.**
3. O **princípio da proporcionalidade** (no sentido mais restrito), que procura evitar **danos a um direito fundamental desproporcionados em relação ao objectivo pretendido**, ou seja, as medidas restritivas dos direitos e liberdades fundamentais não devem, em caso de conflito entre um direito ou liberdade fundamental e o interesse público, exceder, pelas suas consequências negativas, os aspectos positivos do interesse público nestas medidas.

A Directiva de Retenção de Dados e a sua transposição nacional tornaram-se objecto de processos constitucionais em alguns países da UE. As decisões, especialmente dos tribunais constitucionais da

---

Os dados de tráfego e localização são principalmente **dados que levam ao rastreio e identificação da fonte e do destinatário de uma comunicação,** bem como **dados que levam à determinação da data, hora, método e duração da comunicação**.

O âmbito dos dados de tráfego e de localização, a forma e o modo da sua transmissão a organismos autorizados para utilização nos termos de um regulamento legal especial (ver Secção 97 (3) da ECA) e o modo da sua eliminação serão determinados por um instrumento legal legal. O instrumento legal é o **Decreto nº 357/2012 Coll., relativo à conservação, transferência e apagamento de dados de tráfego e de localização.**

Roménia (2009), Alemanha (2010) e República Checa (2011), devem ser mencionadas entre as mais cruciais. Irei concentrar-me nas decisões dos tribunais na Alemanha e na República Checa.

O Tribunal Constitucional Federal da Alemanha resolveu um conflito entre liberdade e segurança (com base na Directiva de Conservação de Dados) e decidiu a favor da liberdade individual. A 2 de Março de 2010, o tribunal decidiu que a retenção em massa de dados sobre telefone e transmissão de dados era inconstitucional na Alemanha.

O tribunal respondeu a uma queixa em massa de 35.000 cidadãos que pediam a revogação de uma lei de 2008 que ordenava às empresas de telecomunicações que arquivassem registos de chamadas telefónicas e comunicações por correio electrónico durante seis meses para fins de investigação. O Tribunal Constitucional Federal revogou os regulamentos contestados com o fundamento de que eram inconstitucionais. Declarou ainda que a obrigação de conservar os dados na medida especificada não é totalmente inconstitucional desde o início, mas não existe um regulamento legal que corresponda ao princípio da proporcionalidade. De acordo com o tribunal, os regulamentos contestados não estavam em conformidade com os requisitos constitucionais de segurança de dados, a finalidade da utilização dos dados (e a transparência da utilização dos dados) não estava claramente definida, e a protecção legal não estava suficientemente assegurada.

O tribunal declarou que *"o exercício dos direitos e liberdades fundamentais dos cidadãos (aqui o sigilo das mensagens transmitidas por meios de comunicação electrónicos) não deve ser completamente controlado, documentado e registado pelo Estado; isto pertence à identidade jurídica constitucional da República Federal da Alemanha, em cuja preservação a república se deve situar a nível europeu e internacional"*.[65]

Na República Checa, a Directiva de Retenção de Dados foi implementada antes da sua entrada em vigor na UE. (Na UE, foi implementada a 15 de Março de 2007, com um requisito de transposição até 15 de Setembro de 2007. Na República Checa, foi implementada na Secção 97/3 da ECA, com efeitos a partir de 1 de Maio de 2005). Foi também apresentada uma queixa constitucional na República Checa, especificamente pela associação Iuricum Remedium, que foi apoiada por um grupo de 51 deputados. Esta queixa foi apresentada ao Tribunal Constitucional em Março de 2010. Em 2011, o Tribunal Constitucional decidiu e deferiu integralmente a petição de anulação total das passagens relevantes da Lei das Comunicações Electrónicas (especificamente a Secção 97 (3) e (4) e o Decreto de Execução n.º 485/2005 Coll., sobre a Extensão dos Dados de Tráfego e Localização e a revogação das disposições do Código de Processo Penal.[66] O Tribunal declarou o seguinte: *"O Tribunal Constitucional considerou que a legislação contestada viola os limites constitucionais porque não satisfaz os requisitos do Estado de direito e viola os requisitos de restrição do direito fundamental à privacidade, sob a forma do direito à autodeterminação informativa na acepção do art. 10 (3) e do art. 13 da Carta, que decorrem do princípio da proporcionalidade"*.

Os legisladores da República Checa responderam às objecções do Tribunal Constitucional da República Checa, e foi adoptada **nova legislação** que continua a permitir a conservação generalizada

---

[65] *O Tribunal Constitucional Federal Alemão rejeita a lei de retenção de dados.* [em linha]. [cit.16/07/2016]. Disponível em: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/
Ver também, por exemplo:
Desafios jurídicos nacionais à Directiva de Retenção de Dados. [em linha]. [cit.16/07/2016]. Disponível em: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
Retenção de dados inconstitucional na sua forma actual. [em linha]. [cit.16/07/2016]. Disponível a partir de: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690
O Bundestag alemão aprova a nova lei de retenção de dados. [em linha]. [cit.16/07/2016]. Disponível em: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/
[66] Ver a decisão do Tribunal Constitucional Pl. ÚS 41/11, em 22/03/2011. *Shromažďování a vyuzívání provozních a lokalizačních údajů o telekomunikačním provozu.* [online]. [cit. 24/08/2016]. Disponível a partir de: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=4&typ=result

de dados de tráfego e localização na República Checa, uma vez que respeita o **teste de proporcionalidade** acima mencionado, em particular declarando claramente a gama de entidades (autorizadas a solicitar dados de tráfego e localização) e a finalidade para a qual os dados podem ser solicitados.

Ao mesmo tempo, foram tomadas medidas ordenando às entidades empresariais que adoptem tais regras ao abrigo da Lei das Comunicações Electrónicas para assegurar que os dados de tráfego e localização sejam da mesma qualidade e sujeitos à mesma segurança e protecção contra acesso não autorizado, alteração, destruição, perda ou roubo ou outro processamento ou utilização não autorizada de dados, de acordo com a Secção 88 da ECA [67]

O comprimento máximo para o qual estes dados podem ser retidos foi também **definido. Actualmente, é de 6 meses.** Após o termo deste período, uma pessoa singular ou colectiva que retenha dados de tráfego e de localização é obrigada a apagá-los, a menos que tenham sido fornecidos a autoridades autorizadas a utilizá-los ao abrigo de legislação especial ou salvo disposição legal em contrário (Secção 90 da ECA). Além disso, **foi estabelecida a obrigação de assegurar que o conteúdo das mensagens não seja retido e entregue durante a conservação dos dados de tráfego e de localização** (Secção 97 (3) da ECA).

Ao mesmo tempo, o Código de Processo Penal enfatiza o **princípio da subsidiariedade** (especialmente os artigos 88 e 88a da Lei n.º 141/1961 Coll., sobre Processos Judiciais Penais): *"se o objectivo pretendido não puder ser alcançado de outra forma ou se a sua realização for significativamente mais difícil"*). A garantia de um mínimo de inteferência com os direitos humanos fundamentais nestes casos é dada, entre outras coisas, pelo facto de a ordem de emissão de dados de tráfego e localização ser emitida por um juiz sob proposta do procurador público.

Quem tem, portanto, o direito de solicitar a divulgação de dados de tráfego e de localização e em que condições na República Checa? Nos termos da Secção 97 (3) da ECA, uma entidade jurídica ou pessoa singular que retenha dados de tráfego e de localização deve disponibilizá-los sem demora mediante pedido:

a) **as autoridades responsáveis pela aplicação da lei** para os fins e em conformidade com as condições estipuladas por um regulamento jurídico especial[68] ,

b) **a Polícia da República Checa** para efeitos de **iniciar uma busca de uma pessoa procurada ou desaparecida específica, identificar uma pessoa de identidade desconhecida ou a identidade de um cadáver encontrado, prevenir ou detectar ameaças específicas no terrorismo ou rastrear uma pessoa protegida** e se as condições estipuladas por um regulamento legal especial forem cumpridas[69] ,

c) **o Serviço de Informação de Segurança** para os fins e em conformidade com as condições estipuladas por um regulamento legal especial[70] ,

d) **Informações militares** para os fins e em conformidade com as condições estipuladas por um regulamento legal especial[71] ,

[67] Para mais detalhes ver a Secção 88a da ECA

[68] Lei n.º 141/1961 Coll., sobre Processos Judiciais Penais (Código Penal), com as alterações que lhe foram introduzidas.

[69] Lei n.º 273/2008 Coll., sobre a Polícia da República Checa, com as alterações que lhe foram introduzidas.
Lei n.º 137/2001 Coll., sobre a protecção especial de uma testemunha e outras pessoas no âmbito de um processo penal e sobre as alterações à Lei n.º 99/1963 Coll., o Código de Processo Civil, com as alterações que lhe foram introduzidas.

[70] Secções 6 a 8 da Lei n.º 154/1994 Coll., sobre o Serviço de Informação de Segurança, com as alterações que lhe foram introduzidas.

[71] Secções 9 e 10 da Lei n.º 289/2005 Coll., sobre Inteligência Militar.

e) **o Banco Nacional Checo** para os fins e em conformidade com as condições estipuladas pela legislação especial[61)72] .

Na União Europeia, o Tribunal de Justiça da UE (em 8 de Abril de 2014) emitiu um veredicto na sequência do anterior parecer do[73] seu Advogado-Geral Pedro Cruz Villalón[74] , no qual **anulou a Directiva de Retenção de Dados relevante (2006/24/CE**).

> *"Pelo acórdão de hoje, o Tribunal de Justiça declara a directiva inválida".*
>
> *"Dado que o Tribunal de Justiça não limitou os efeitos temporais do acórdão, a declaração de nulidade produz efeitos a partir da data de entrada em vigor da directiva".*

Em particular, o Tribunal de Justiça da UE criticou o facto de *"o legislador da UE ter excedido os limites estabelecidos pela exigência de conformidade com o princípio da proporcionalidade ao adoptar a Directiva de Retenção de Dados".*

A decisão de manter ou revogar a legislação existente que rege a conservação de dados de tráfego e localização nos Estados-Membros da UE cabe inteiramente às autoridades nacionais relevantes, e a própria União Europeia não pretende recomendar ou fornecer qualquer orientação sobre como agir [75]

Como abordar a retenção generalizada dos dados de tráfego e localização? Pessoalmente, acredito que, no ciberespaço, não é possível reconstruir eventos que tiveram lugar no passado a não ser através da retenção de dados de tráfego e localização. O ciberespaço e as TIC, que permitem uma mudança muito rápida na topologia da rede, serviços, etc., tecnologias que permitem a aquisição de várias identidades diferentes em segundos, de facto, não permitem qualquer outra opção.

Estou ciente de que a retenção generalizada de dados de tráfego e localização interfere com os meus direitos e liberdades fundamentais. Contudo, ao adoptar o conceito de contrato social e ao renunciar a parte dos meus direitos e liberdades em favor de uma autoridade (no nosso caso o Estado) para me proteger a mim e aos meus direitos, não tenho, de facto, outra escolha. Creio que, se quisermos verificar e investigar eficazmente a cibercriminalidade, os ciberataques e outros fenómenos negativos que ocorrem no ciberespaço, não o poderemos fazer sem esta ferramenta. A questão que devemos abordar não o deve ser: *"Como limitar a recolha de dados e informações sobre pessoas no ciberespaço (porque isto acontece a níveis completamente diferentes) e assim limitar a capacidade do Estado para abordar fenómenos negativos no ciberespaço"?* As questões que são completamente legítimas e que devem ser abordadas são: *"Como estabelecer as regras, a quem e em que condições permitir o acesso aos dados, o que acontece aos dados, para que fins podem ser utilizados, etc.".*

Pessoalmente, acredito que dados semelhantes devem ser retidos não só pelos fornecedores de serviços públicos, mas também por todos os ISP que fornecem um serviço. A minha opinião fundamenta-se nas seguintes razões.

Em primeiro lugar, acredito que outros serviços que não os baseados no fornecimento de ligações são e continuarão a ser a maioria dos serviços no ciberespaço. Assim, um utilizador deixa de abordar a questão de quem o liga e como e está principalmente envolvido em serviços que podem, por exemplo,

---

[72] Lei n.º 15/1998 Coll., sobre a Supervisão na Área do Mercado de Capitais e sobre Alterações a Outras Leis, com as alterações que lhe foram introduzidas.

[73] Conclusões do Advogado-Geral Pedro Cruz Villalón Processo C-293/12 e C-594/12. [em linha]. [cit.15/07/2016]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

[74] O Tribunal de Justiça da União Europeia. Comunicado de imprensa n.º 54/14, datado de 8 de Abril de 2014. **Acórdão nos processos apensos C-293/12 e C-594/12**. [em linha]. [citado 15/07/2016]. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

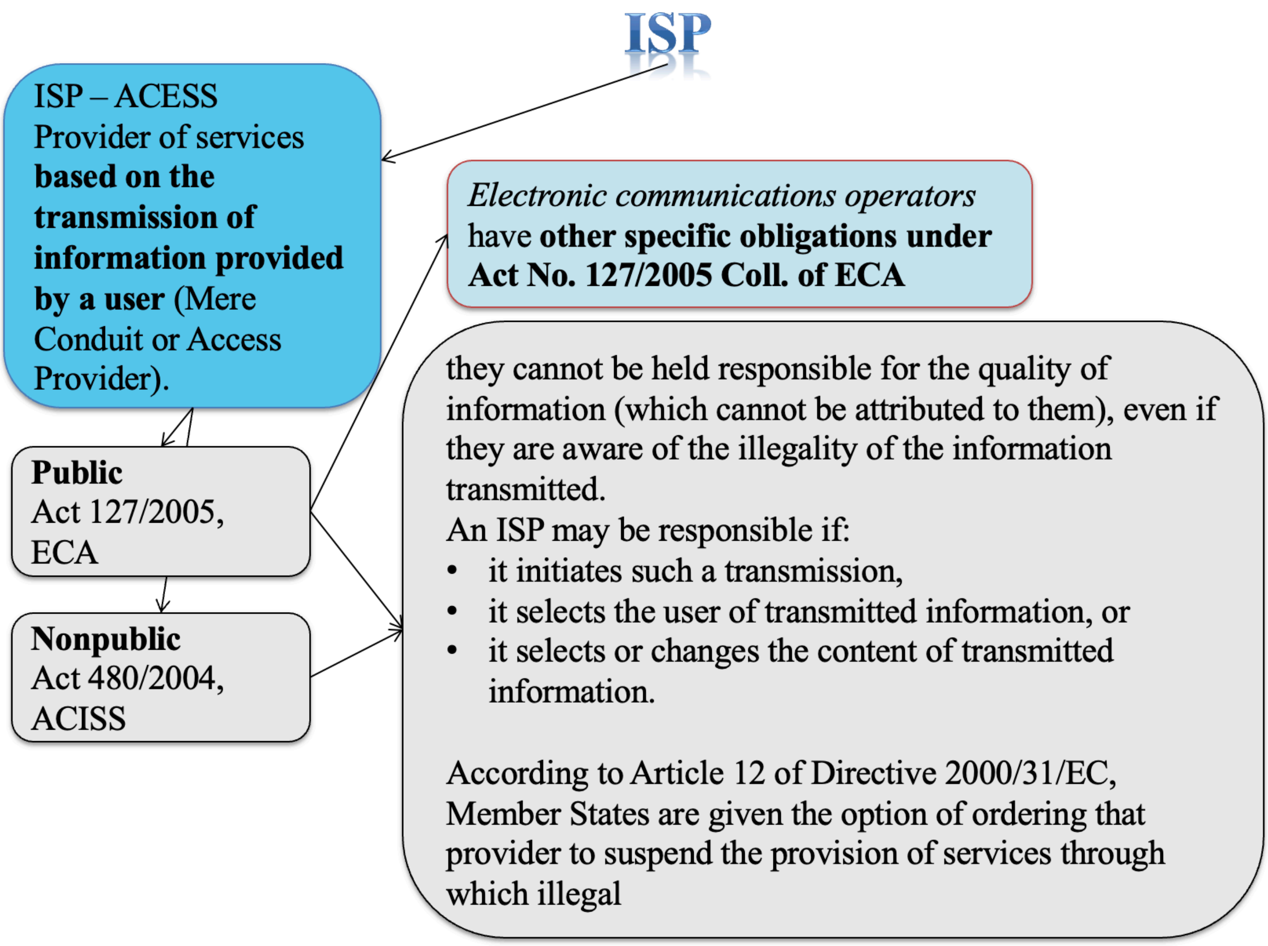
[75] PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám uz uz EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10/11/2015]. Disponível em: http://www.earchiv.cz/b14/b0428001.php3

tomar a forma de uma ligação virtual a vários ambientes virtuais. Assim, não é a ligação física em si que será significativa, mas sim a ligação entre os serviços individuais.

A segunda razão é o facto de a grande maioria dos fornecedores destes serviços já reter não só os dados de tráfego e de localização, mas também uma série de outros dados que os utilizadores lhes permitem reter com base nos Termos de Serviço acordados por um utilizador final em relação a um ISP.

A última razão é a própria protecção de um ISP contra os utilizadores. Um prestador de serviços deve respeitar a lei, e é do seu melhor interesse reter dados que possam potencialmente isentá-lo de responsabilidade, por exemplo, por danos ou outros danos.

Um Advogado-Geral comentou recentemente sobre a retenção de dados de tráfego e localização[76] . Observou que a retenção de dados é, em muitos casos, a única ferramenta eficaz para lidar com os riscos de segurança e crimes graves. Ao mesmo tempo, formulou requisitos para a sua implementação proporcional nos sistemas jurídicos dos Estados Membros.



Representação gráfica da divisão dos fornecedores de ligação e de alguns dos seus direitos e obrigações

[76] Conclusões do Advogado-Geral SAUGMANDSGAARD ØE, de 19/07/2016. Nos processos apensos C-203/15 e C-698/15. [em linha]. [citado 10/8/2016]. Disponível a partir de: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

3.1.2 Prestadores de serviços baseados no armazenamento automático intermédio de informações fornecidas por um utilizador (o chamado caching)

O cache é baseado na transferência de informação, durante a qual é automaticamente armazenada temporariamente. Subsequentemente, esta informação é transmitida aos destinatários do serviço, a seu pedido.

"O cache é basicamente um arranjo especial do mero serviço de condutas, uma vez que também inclui transmissão com armazenamento intermédio temporário de informação. A única diferença em que o serviço de cache poderia desviar-se do âmbito de um mero conduto amplamente concebido é que o armazenamento durante a transmissão é efectuado por um "período mais longo do que o razoavelmente necessário para a transmissão".[77]

Husovec também descreve muito apropriadamente os serviços de cache no exemplo de um servidor proxy ou navegador de cache, que aceleram o carregamento de páginas web. Um destinatário do serviço é proprietário de um website de notícias diárias (o chamado destinatário primário), cujas imagens são guardadas por um fornecedor de cache num computador geograficamente mais próximo (por exemplo, na Europa) para que não tenha de aceder constantemente ao computador onde o website original é armazenado (por exemplo, África). Consequentemente, a carga global da página (na Europa) é acelerada. Um utilizador que visita o sítio web e é outro destinatário do serviço (o chamado destinatário secundário), assim, com base num pedido individual dirigido ao fornecedor do serviço de cache, obtém uma imagem do seu computador e não é obrigado a "viajar" para o computador original. [78]

Os fornecedores de cache não estão isentos de responsabilidade pela qualidade da informação se violarem a norma ou as condições técnicas acordadas de cache.[79]

De acordo com a Secção 4 do ACISS, um fornecedor de cache é responsável se o mesmo:

a) altera o conteúdo da informação,
b) não preenche as condições de acesso à informação,
c) não cumpre as regras de actualização de informações geralmente reconhecidas e utilizadas no sector em causa,
d) exceder a utilização permitida de tecnologia geralmente reconhecida e utilizada na indústria para obter dados de utilização; ou
e) não tomará medidas imediatas para remover ou negar o acesso à informação que armazena logo que verifique que a informação foi removida ou acedida da rede no ponto de transmissão ou que foi ordenada por um tribunal a retirar ou negar o acesso à mesma.

Um fornecedor de cache não é obrigado a procurar activamente factos e circunstâncias que apontem para o conteúdo ilegal da informação ou a supervisionar o conteúdo da informação transmitida ou armazenada por ele.

---

[77] ver HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praga: CZ.NIC, 2014, p. 133
[78] Ibidem, p. 133.
[79] Cf. artigo 13º da Directiva 2000/31/CE e as disposições da Secção 4 do ACISS
Cf. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 58

3.1.3 Prestadores de serviços baseados no armazenamento de informações fornecidas por um utilizador (o chamado armazenamento ou alojamento)

Fornecer armazenamento ou alojamento significa disponibilizar armazenamento (espaço) a um utilizador para que este possa ali colocar os dados. O armazenamento de informação ou dados, ao contrário do mero conduíte ou caching, não é apenas temporário. Os serviços de alojamento incluem:

a) Webhosting (Active 24, Ignum, Zoner, etc.)

b) Armazenamento em nuvem que permite o armazenamento de quaisquer ficheiros e dados (Dropbox, iCloud, Microsoft OneDrive, ownCloud, etc.)

c) Armazenamento de ficheiros (Rapidshare, DropBox, etc.)

d) Armazenamento de vídeo (YouTube, etc.)

e) Armazenamento de ficheiros áudio (iTunes, etc.)

f) Serviços de leilão na Internet (eBay, etc.)

g) Blogs, fóruns, chats de discussão, etc.

h) Meios de comunicação social (Facebook, Twitter, etc.).

A lista acima não é definitiva. Vários outros serviços podem ser fornecidos dentro de um alojamento.

Para os fornecedores de alojamento, a situação com a sua possível responsabilidade legal é a mais complicada.[80] Mais uma vez, baseia-se nas disposições da Directiva nº 2000/31/CE, cujas recomendações foram adoptadas pelo legislador checo na Secção 5 do ACISS. Esta disposição estipula pelo menos a negligência involuntária de um fornecedor[81] em relação a um conteúdo ilegal de informação armazenada pelo fornecedor. Contudo, **o legislador não obriga os fornecedores a procurar activamente informações ilegais dos utilizadores**[82] (porque, em muitos casos, seria efectivamente uma interferência com os direitos e liberdades fundamentais garantidos pela Carta - por exemplo, o artigo 13º) ou a supervisionar o conteúdo das informações transmitidas ou armazenadas.

De acordo com a Secção 5 (1) do ACISS, um fornecedor de alojamento será responsável se o mesmo:

a) ***poderia, em relação ao objecto da sua actividade e às circunstâncias e natureza do caso, saber que o conteúdo da informação armazenada ou da acção do utilizador é ilegal****, ou*

b) ***tendo comprovadamente obtido conhecimento da natureza ilegal das informações armazenadas ou da acção ilegal do utilizador,*** *não tomou, sem demora, todas as medidas, que poderiam ser necessárias, para remover ou impossibilitar o acesso a tais informações.*

Um fornecedor de alojamento será sempre responsável pelo conteúdo da informação armazenada se esta exercer, directa ou indirectamente, uma influência decisiva sobre a actividade do utilizador.[83]

Para efeitos desta monografia, foram seleccionados apenas alguns aspectos relacionados com os prestadores de serviços da sociedade da informação, em particular no que diz respeito à usabilidade da informação na detecção e investigação de cibercrimes e ciberataques.

[80] Cf. artigo 14º da Directiva 2000/31/CE e as disposições da Secção 5 do ACISS
[81] Cf. disposições da Secção 16 (1) (b) do Código Penal.
[82] Cf. artigo 15º da Directiva 2000/31/CE e as disposições da Secção 6 do ACISS
[83] Secção 5 (2) do ACISS

3.2 Regulamentação das actividades dos ISP na Polónia

Na Polónia, a lei que regula a Lei de 18 de Julho de 2002 sobre a prestação de serviços electrónicos (Journal Of Laws of 2002 No. 144, item 1204), que limita grandemente os casos em que um ISP pode ser considerado responsável:

Arte. 12. 1. O prestador de serviços que fornece serviços por meios electrónicos, incluindo a transmissão de dados transmitidos pelo destinatário do serviço na rede de telecomunicações ou o fornecimento de acesso à rede de telecomunicações na acepção da Lei de 16 de Julho de 2004 - Lei das Telecomunicações, não será responsável pelo conteúdo destes dados, se:

1) não é o iniciador da transferência de dados;

2) não selecciona o destinatário da transferência de dados;

3) não selecciona nem modifica a informação contida na mensagem.

2. A exclusão de responsabilidade referida no parágrafo. 1 também inclui o armazenamento automático e indirecto a curto prazo dos dados transmitidos, se esta actividade for exclusivamente para efeitos de transmissão e se os dados não forem armazenados por mais tempo do que o normalmente necessário para efectuar a transmissão.

Arte. 13. 1. A pessoa que transmite os dados e fornece o armazenamento automático e intermediário a curto prazo destes dados, a fim de acelerar o re-acesso aos mesmos, com base no pedido Art. de outra entidade:

1) não modifica os dados;

2) utiliza técnicas informáticas reconhecidas e habitualmente utilizadas neste tipo de actividade, que definem os parâmetros técnicos de acesso aos dados e a sua actualização, e

3) não interfere com a utilização de técnicas informáticas reconhecidas e normalmente utilizadas neste tipo de actividade no domínio da recolha de informações sobre a utilização dos dados recolhidos.

2. A pessoa que, nas condições referidas no parágrafo. 1, apagará imediatamente os dados ou impedirá o acesso aos dados armazenados, quando obtiver a mensagem de que os dados foram removidos da fonte de transmissão original ou de que o acesso aos mesmos foi tornado impossível, ou quando um tribunal ou outra autoridade competente tiver ordenado que os dados sejam apagados ou impedidos de serem acedidos. Art. 14. 1. Nenhuma responsabilidade pelos dados armazenados será assumida por quem, ao mesmo tempo que fornece os recursos do sistema TIC para efeitos de armazenamento de dados pelo destinatário do serviço, não tem conhecimento da natureza ilícita dos dados ou actividades relacionadas, e no caso de receber uma notificação governamental ou obter informações fiáveis sobre a natureza ilícita dos dados ou actividades relacionadas, impedirá imediatamente o acesso a esses dados.

2. O prestador de serviços que tenha recebido uma notificação oficial da natureza ilegal dos dados armazenados fornecidos pelo destinatário e tenha impedido o acesso a esses dados, não é responsável por este destinatário por danos resultantes de impedir o acesso a esses dados.

3. O prestador de serviços que tenha obtido informações credíveis sobre a natureza ilícita dos dados armazenados fornecidos pelo destinatário do serviço e que tenha impedido o acesso a esses dados, não é responsável perante esse destinatário de serviços por danos resultantes de impedir o acesso a esses dados, se notificar de imediato o destinatário da intenção de impedir o acesso aos mesmos.

4. As disposições do parágrafo. 1-3 não se aplicam se o prestador de serviços tiver assumido o controlo do destinatário na acepção das disposições relativas à concorrência e à protecção dos consumidores.

Arte. 15. A entidade que presta os serviços especificados no art. 15º. 12-14, não é obrigada a verificar os dados transferidos, armazenados ou disponibilizados por ele, a que se refere o artigo 1. 12–14

3.3 Regulamentação das actividades dos ISP em Portugal

Conserte-me

3.4 Possibilidades de responsabilidade legal de um utilizador por acções no ciberespaço

Muitos utilizadores de sistemas de informação e comunicação desconhecem a sua potencial responsabilidade pela utilização indevida destas tecnologias.[84] Os sistemas de informação e comunicação são uma coisa, e a pessoa que os manuseia é obrigada a **agir de tal forma que não haja danos injustificados à liberdade, vida, saúde ou propriedade de outrem.**[85]

Se um delinquente causar danos a uma parte lesada, violando intencionalmente os bons costumes, é obrigado a indemnizar essa parte; no entanto, se exercer o seu direito, o delinquente só é obrigado a indemnizar o dano se observar o dano de outra como objectivo principal.[86]

Esta redacção do Código Civil implica claramente tanto a obrigação de gerir adequadamente os sistemas de informação e comunicação, como a obrigação de evitar danos que possam surgir das suas actividades (ou seja, a utilização das TIC no ambiente da Internet).

Muitos utilizadores comuns subestimam a protecção e segurança dos recursos TIC à sua disposição, quer negligentemente, quer intencionalmente.

A determinação da forma de culpa nas acções de um utilizador final é crucial para uma possível responsabilidade civil ou criminal. Esta afirmação pode ser demonstrada em três casos ilustrativos do mundo real.

Um utilizador de computador pessoal estava a utilizar uma cópia ilegal do sistema operativo Windows 7 e, intencionalmente, não actualizou o sistema. O utilizador instalou intencionalmente programas no computador que permitiram a terceiros manipular o computador sem a sua ajuda adicional.

O objectivo da actividade do utilizador acima descrita era libertar-se de qualquer responsabilidade criminal por um ataque efectuado por outra pessoa num computador tão preparado (por exemplo, o computador faz intencionalmente parte de uma rede de botnets).

Na prática, é possível encontrar tais atacantes que baseiam a sua defesa no facto de não terem sido eles a pessoa que levou a cabo um ataque específico através de um computador.

Evitar a culpa com base na alegação de que a pessoa não é um atacante directo e as suas acções não causaram um ataque específico não é, na minha opinião, legítimo, ou não é válido aceitar absolutamente esta alegação.

Do ponto de vista do direito penal, pelo menos a aplicação da instituição de participação e do princípio de acesso à participação poderia ser considerada[87] uma vez que os actos de uma pessoa que ajudou e foi cúmplice de uma infracção penal por outra (em particular, **fornecendo os meios, removendo as barreiras**, levando a pessoa lesada ao local do crime, vigiando enquanto um acto foi cometido, aconselhando, encorajando a determinação ou prometendo participar numa infracção penal) podem ser subsumidos ao abrigo das disposições sobre um acessório.[88] Neste caso, fornecer os meios significaria também disponibilizar um sistema informático, ou parte dele, para a prática de uma

---

[84] Para esta parte do texto foram utilizadas teses que foram parcialmente publicadas no artigo: KOLOUCH, Jan e Andrea KROPÁČOVÁ. Responsabilidade pelo Dispositivo Próprio e Dados e Aplicações nele Armazenados. In: *Avanços na Ciência da Informação e Aplicações Volume I: Actas da 18ª Conferência Internacional sobre Computadores (parte do CSCC '14).* [B.m.], c2014, pp. 321-324. Série Avanços Recentes em Engenharia Informática, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

[85] Secção 2900 do Código Civil

[86] Secção 2909 e seguintes do Código Civil

[87] Este é o princípio da dependência da responsabilidade penal e da criminalidade do participante (ver Secção 24 do Código Penal) da responsabilidade penal e da criminalidade do principal infractor (ver Secção 22 do Código Penal), desde que o principal infractor tenha pelo menos tentado cometer uma infracção penal em que o participante tenha participado.

[88] Sob a condição de um acordo entre o participante e o principal infractor. Ver Secção 24 (1) (c) do Código Penal

infracção penal intencional.

Se fosse provado um maior grau de participação directa de um utilizador na infracção de outra pessoa, seria possível considerar esse utilizador como cúmplice[89] numa infracção penal. O factor decisivo seria o nível de conhecimento sobre a utilização de um determinado computador para um acto ilegal e a compreensão adicional de que esta actividade pode violar ou pôr em perigo os interesses protegidos pelo direito penal.[90]

Do ponto de vista do direito civil, as acções de tal utilizador poderiam ser incluídas no artigo 2909 do Código Civil, ou seria possível utilizar o artigo 2915 do Código Civil, que regula o caso em que o dano é causado por várias pessoas. Esta disposição estipula que: *"se vários delinquentes forem obrigados a indemnizar, devem fazê-lo conjunta e solidariamente; se qualquer dos delinquentes tiver o dever, ao abrigo de outro estatuto, de indemnizar apenas até um certo limite, é obrigado a fazê-lo conjunta e solidariamente com os outros delinquentes nessa medida.* ***Isto também se aplica quando várias pessoas cometeram actos ilícitos separados, cada um dos quais pode ter causado uma consequência prejudicial com um elevado grau de certeza e se a pessoa que causou o dano não puder ser identificada. "***É a segunda frase da Secção 2915 (1) que, na minha opinião, pode ser muito bem aplicada ao caso acima descrito.

Um utilizador de computador pessoal estava a utilizar uma cópia ilegal do sistema operativo Windows 7 e, intencionalmente, não actualizou o sistema. Tinha uma série de jogos e outras aplicações instaladas no seu computador, nas quais foi cometida uma violação dos direitos de autor, em particular contornando ou suprimindo elementos da sua protecção e utilizando keygens ou cracks[91] *que continham malware de outros atacantes. O utilizador não estava ciente de que o seu computador estava a ser utilizado por outros utilizadores.*

Na prática, este é o caso mais comum em que um computador é mal utilizado sem o conhecimento do seu utilizador autorizado, mesmo que esse utilizador, através da sua má conduta (especialmente violação dos direitos de autor) ou simples ignorância da tecnologia informática, tenha feito com que o seu computador fosse mal utilizado para atacar terceiros.

Do ponto de vista do direito penal, não é possível utilizar a instituição da participação e o princípio da participação acessória neste caso, porque os actos da pessoa que permitiu ou facilitou a prática de uma infracção penal por outra pessoa não foram intencionais e, portanto, não tiveram por objectivo ajudar o principal infractor.

Do ponto de vista da culpabilidade, seria possível aplicar ao utilizador de um computador infectado as disposições relativas à negligência não desejada, uma vez que o infractor não sabia que a sua conduta poderia causar tal violação ou pôr em perigo, embora pudesse e devesse ter tido conhecimento disso, tendo em conta as circunstâncias e as relações pessoais.[92]

Devido ao facto de não haver uma natureza factual negligente do crime no Código Penal, de acordo com a Secção 230: *Acesso não autorizado a sistemas informáticos e meios de informação*, não será possível utilizar os institutos de direito penal neste caso particular.

Do ponto de vista do direito civil, a conduta de um tal utilizador poderia então ser subsumida ao abrigo da Secção 2912 (1) do Código Civil: *"Se um delinquente agir de forma diferente do que se pode razoavelmente esperar em negócios privados de uma pessoa de qualidades médias, presume-se que está a agir de forma negligente".* A este respeito, deve recordar-se que a pessoa que causou o dano

[89] Ver Secção 23 do Código Penal
[90] Ver Secção 15 (1) (b) do Código Penal
[91] Trata-se de intervenções em programas por outras pessoas com o objectivo de modificação com vista a um lançamento mais fácil (keygens), paralisando as protecções do programa que impedem a sua cópia ou lançamento em condições pré-determinadas (fendas) e posterior reformulação destes programas para posterior utilização ou distribuição a outras pessoas.
[92] Ver Secção 16 (1) (b) do Código Penal

(tortfeasor) é obrigada a compensar o dano, independentemente da sua culpa nos casos previstos por lei.[93]

Um utilizador "cuida" adequadamente do seu computador (tem software legal, actualiza-o, etc.) e protege-o razoavelmente (utiliza protecção e verificações antivírus, antispam e anti-malware), mas este computador foi atacado do exterior (por exemplo, ligado a uma botnet) e subsequentemente utilizado para atacar outro.

Considero que, do ponto de vista da culpa, não seria possível, neste caso, que os utilizadores de um computador infectado deste tipo estivessem sujeitos mesmo às disposições relativas à negligência não desejada. Devido à actividade proactiva de tal utilizador, a aplicação da Secção 232 do Código Penal está também fora de questão: Os *danos aos Sistemas Informáticos e aos Registos dos Meios de Informação e a Interferência com Equipamento Informático por Negligência,* como negligência grosseira, são exigidos nesta disposição.[94]

Do ponto de vista do direito civil, então, a conduta de tal utilizador não seria, na minha opinião, possível de ser subsumida ao abrigo do anteriormente mencionado artigo 2912 (1) do Código Civil, pois neste caso o utilizador agiu como justificadamente lhe foi exigido. Contudo, isto tem de ser entendido de forma mais ampla, porque, se um utilizador souber que os seus recursos TIC estão a ser indevidamente utilizados para atacar outro, é obrigado a notificar essa pessoa que pode ser prejudicada em resultado deste facto sem demora indevida[95] e a avisar essa pessoa das possíveis consequências. Se cumprir a obrigação de notificação, a pessoa lesada não tem direito a indemnização pelos danos que poderia ter evitado após a notificação.[96]

Num caso específico, dependerá sempre de todas as circunstâncias do caso, e só o tribunal tem o direito de estipular a obrigação de pagamento de indemnizações.

Por outro lado, se um utilizador não "cuida" do seu computador (ou seja, não o assegura, não efectua a manutenção, etc.) e é posteriormente utilizado indevidamente, é realista que o tribunal, em processos de indemnização, imponha uma obrigação a esse utilizador em parte ou na totalidade (por exemplo, de utilizar o poder informático de um centro de dados) de compensar a parte lesada pelos danos que lhe são causados pelo computador do utilizador.

[93] Ver Secção 2895 do Código Civil

[94] Ver Secção 16 (2) do Código Penal: *"Uma infracção penal é cometida por negligência grave se a abordagem de um infractor aos requisitos de diligência devida demonstrar uma evidente irresponsabilidade do infractor relativamente aos interesses protegidos pelo Código Penal".*

[95] A questão é se é possível identificar realisticamente tal pessoa num dado momento (momento de ataque).

[96] Ver secção 2092 do Código Civil

RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

- As autoridades definidoras participam na criação da lei na Internet, na restrição ou expansão das suas actividades, através da criação de normas definidoras.
- A definição de normas é criada e implementada por entidades autorizadas a definir o ambiente da rede de informação. Na prática, estas são normas *sui generis* que definem redes de informação como tal. Ocorrem em camadas que são interdependentes. *"A definição de normas são criadas por operadores de telecomunicações, produtores de software de escritório mas também, por exemplo, criadores ou operadores de jogos online, ou qualquer pessoa que abra um blogue ou tenha uma caixa de correio electrónico, (Uma norma definidora criada por um utilizador desta caixa é um filtro que executa automaticamente uma operação de caixa de entrada definida)"*.
- As autoridades definidoras são os criadores das normas definidas. É uma entidade que, através do seu funcionamento, cria regras para o funcionamento do sistema lógico em que a autoridade opera. Como mencionado anteriormente, a ICANN tem uma posição executiva entre estas autoridades, uma vez que é responsável pela atribuição, administração e estabelecimento de regras para o sistema de nomes de domínio. Outra autoridade definidora é, por exemplo, a IETF. Embora as autoridades definidoras possam parecer ser administradores ilimitados do ciberespaço, continuam a estar sujeitas à lei de um Estado.
- A Internet só existe graças à definição das autoridades. É composta por elas. Nenhuma operação terá lugar sem a participação (execução ou mediação da operação) da autoridade definidora.
- O ciberespaço é formado pela vontade de definir autoridades.
- Todos os prestadores de serviços da sociedade da informação estão a definir autoridades.
- Todos os prestadores de serviços, como qualquer outro organismo de direito, são legalmente responsáveis pelas suas acções.
- O termo ISP é também definido na Convenção sobre o Cibercrime, especificamente no artigo 1 (c) onde se afirma que o fornecedor de serviços é:
    - qualquer entidade pública ou privada que forneça aos utilizadores do seu serviço a capacidade de comunicar por meio de um sistema informático e
    - qualquer outra entidade que processe ou armazene dados informáticos em nome de tal serviço de comunicação ou utilizadores de tal serviço.
- A Lei checa sobre certos serviços da sociedade da informação reconhece os três prestadores de serviços seguintes, estipulando que um prestador de serviços é qualquer pessoa singular ou colectiva que preste qualquer um dos serviços da sociedade da informação: [97]
    - Prestadores de serviços baseados na transmissão de informações fornecidas por um utilizador (Mere Conduit ou Access Provider).
    - Prestadores de serviços baseados no armazenamento automático intermédio de informações fornecidas por um utilizador (o chamado caching).
    - Prestadores de serviços baseados no armazenamento de informação fornecida por um utilizador (o chamado armazenamento ou hosting).

[97] Ver Secção 2 (d) do ACISS

PALAVRAS-CHAVE A LEMBRAR

- ISP
- Definindo a autoridade
- Definindo o padrão
- Mero condutor ou fornecedor de acesso
- Fornecedor de caixa
- Fornecedor de alojamento
- Retenção de dados

PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- Definir ISP.
- Como estão divididos os ISPs? De acordo com que critérios?
- Quais são as responsabilidades dos ISPs?
- O que é uma norma de definição?
- Quem é uma autoridade definidora, e qual é o seu papel?
- O que é a retenção de dados?

4. A ciber-segurança e a sua regulamentação legal

Os esforços para abordar a ciber-segurança podem ser vistos com efeito desde o início da utilização das tecnologias de informação e comunicação. Gradualmente, foram adoptadas recomendações, normas ou normas técnicas nesta área, que geralmente definiam requisitos mínimos que garantiam um certo nível de segurança.

Há muitas razões para a introdução e implementação da ciber-segurança. As mais comuns incluem, por exemplo, consequências económicas negativas no caso de um ciberataque bem sucedido em que os dados sensíveis são roubados. Um ciberataque bem sucedido pode também comprometer as próprias operações e o funcionamento de uma organização, por exemplo, restringindo o acesso a sistemas informáticos ou a dados através de resgates. Outra razão para a introdução da ciber-segurança pode também ser a perda de credibilidade de uma organização atacada, etc.

A última mas não menos importante razão para a implementação da ciber-segurança é cumprir os regulamentos legais, bem como os direitos e obrigações decorrentes destes regulamentos. Esta razão legislativa para muitos assuntos deriva da Lei de Segurança Cibernética, mas é errado assumir que esta é a única norma legal relacionada com a questão da segurança cibernética.

Nos últimos anos, especialmente, tem havido um aumento maciço da legislação internacional que se concentra especificamente nas actividades de entidades (indivíduos, entidades jurídicas ou estados e outras organizações) no ciberespaço.

O campo da ciber-segurança difere significativamente de outras áreas onde os princípios de segurança padrão são aplicados no mundo real. A diferença reside principalmente na possibilidade de desenvolvimento dinâmico e mudança imediata de ciberataques e ameaças (a maioria das ameaças no mundo real permanecem relativamente constantes), o que pode acarretar certos problemas em relação à legislação. A regulamentação legal nesta área deve, por um lado, ser suficientemente geral para lhe permitir responder eficazmente a fenómenos cibernéticos parcialmente negativos sem a necessidade da sua especificação detalhada, mas, por outro lado, não deve ser demasiado vaga para não infringir os direitos e interesses legítimos dos indivíduos em maior medida do que é estritamente necessário.

Antes da análise real da legislação existente válida e eficaz no domínio da ciber-segurança, deve notar-se que, dentro e fora da União Europeia, há um esforço claro para implementar instrumentos legais mais eficazes que aumentariam a qualidade da ciber-segurança e permitiriam uma resposta adequada às ameaças e ataques cibernéticos. Actualmente, as inconsistências e deficiências nas normas legais dos Estados-Membros da UE e de outros Estados que decidiram participar activamente na criação da ciber-segurança estão a ser gradualmente eliminadas.

"Os métodos de protecção de dados e sistemas de informação são hoje objecto de muitos estudos científicos. No entanto, sem uma base jurídica, a protecção técnica destes sistemas e dados pode ser ineficaz devido à definição pouco clara de até onde é possível ir com tal protecção. *Neste contexto, a inconsistência dos regulamentos legais de cada Estado com os regulamentos legais de outros Estados manifesta-se plenamente. Devido ao desenvolvimento das tecnologias informáticas e de informação, que ilustram a natureza internacional do cibercrime, a protecção eficaz dos sistemas informáticos e dos dados é impensável sem a existência de um quadro jurídico internacional ou transnacional, tanto entre os Estados-Membros da UE como a nível mundial".*[98]

Este capítulo abordará o quadro legislativo para a ciber-segurança na UE e nos países parceiros que participam no projecto Erasmus+.

---

[98] KOLOUCH, Jan e Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praga: Academia de Polícia da República Checa em Praga, 2013, p. 65

4.1 Documentos UE/CE utilizados para harmonizar a legislação em matéria de ciber-segurança

As redes e os sistemas e serviços de informação desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais para as actividades económicas e sociais, e em particular para o funcionamento do mercado interno.

A magnitude, frequência e impacto dos incidentes de segurança estão a aumentar, e representam uma grande ameaça para o funcionamento da rede e dos sistemas de informação. Estes sistemas podem também tornar-se alvo de acções prejudiciais deliberadas destinadas a danificar ou interromper o funcionamento dos sistemas. Tais incidentes podem impedir a prossecução de actividades económicas, gerar perdas financeiras substanciais, minar a confiança dos utilizadores e causar grandes danos à economia da União Europeia.

As redes e os sistemas de informação, e principalmente a Internet, desempenham um papel essencial para facilitar a circulação transfronteiriça de bens, serviços e pessoas. Devido a essa natureza transnacional, perturbações substanciais desses sistemas, intencionais ou não intencionais e independentemente do local onde ocorram, podem afectar os Estados-Membros individuais e a União Europeia como um todo. A segurança das redes e dos sistemas de informação é, portanto, essencial para o bom funcionamento do mercado interno.

Com base nos progressos significativos realizados no âmbito do Fórum Europeu dos Estados-Membros para promover debates e intercâmbios sobre boas práticas políticas, incluindo o desenvolvimento de princípios para a cooperação europeia em matéria de cibercrise, deverá ser criado um Grupo de Cooperação, composto por representantes dos Estados-Membros, da Comissão e da Agência da União Europeia para a Segurança das Redes e da Informação ("ENISA"), para apoiar e facilitar a cooperação estratégica entre os Estados-Membros em matéria de segurança das redes e dos sistemas de informação. Para que esse grupo seja eficaz e inclusivo, é essencial que todos os Estados-Membros tenham capacidades mínimas e uma estratégia que garanta um elevado nível de segurança das redes e dos sistemas de informação no seu território. Além disso, os requisitos de segurança e notificação devem aplicar-se aos operadores de serviços essenciais e aos fornecedores de serviços digitais para promover uma cultura de gestão de riscos e assegurar que os incidentes mais graves sejam comunicados.[99]
Em particular, devido à natureza específica do ciberespaço sem fronteiras e à necessidade de uma cooperação internacional eficaz, a UE procura aproximar a legislação de cada Estado-Membro para que a ciber-segurança possa ser combatida eficazmente.

Regulamentos, directivas, decisões-quadro e outros documentos da UE/CE são principalmente um meio de aproximar as leis de cada país da UE. Em termos de ciber-segurança, os documentos mais importantes são os seguintes:

Direito primário da UE

- Carta dos Direitos Fundamentais da União Europeia

Directivas do Parlamento Europeu e do Conselho

- 91/250/CEE sobre a protecção jurídica dos programas de computador
- 98/34/CE relativa ao procedimento de informação no domínio das normas e regulamentações técnicas, com a redacção que lhe foi dada pela Directiva 98/48/CE

[99] https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

- 1999/5/CE relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade
- 2000/31/CE relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (Directiva sobre o comércio electrónico)
- 2002/19/CE relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos (Directiva Acesso)
- 2002/20/CE relativa à autorização de redes e serviços de comunicações electrónicas (Directiva Autorização), com a redacção que lhe foi dada pela Directiva 2009/140/CE
- 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (directiva-quadro), com a redacção que lhe foi dada pela Directiva 2009/140/CE
- 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (Directiva Serviço Universal)
- 2002/58/CE sobre o tratamento de dados pessoais e a protecção da privacidade no sector das comunicações electrónicas
- 2006/24/CE relativa à conservação de dados gerados ou tratados no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações
- 2008/114/CE sobre a identificação e designação das infra-estruturas críticas europeias e a avaliação da necessidade de melhorar a sua protecção
- 2011/93/UE relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil, em substituição da Decisão-Quadro 2004/68/JAI do Conselho
- 2013/11/UE relativa aos modos alternativos de resolução de litígios em matéria de consumo e que altera o Regulamento (CE) n.º 2006/2004 e a Directiva 2009/22/CE (Directiva relativa aos modos alternativos de resolução de litígios em matéria de consumo)
- 2013/40/EU sobre ataques aos sistemas de informação e em substituição da Decisão-Quadro 2005/222/JAI do Conselho
- 2015/1535 sobre o procedimento para o fornecimento de informações no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação
- 2015/2366 relativa aos serviços de pagamento no mercado interno, que altera as Directivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Directiva 2007/64/CE ("Directiva revista relativa aos serviços de pagamento")
- 2016/680 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou de execução de sanções penais, à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho
- **2016/1148 sobre medidas para um elevado nível comum de segurança das redes e sistemas de informação em toda a União Europeia (NIS)**

Regulamentos do Parlamento Europeu e do Conselho

- 460/2004/CE que cria a Agência Europeia para a Segurança das Redes e da Informação, com a redacção que lhe foi dada pelo Regulamento n.º 1007/2008

- 1077/2011/CE que cria uma Agência Europeia de Gestão Operacional dos Sistemas de Informação de Grande Escala no Espaço de Liberdade, Segurança e Justiça
- 526/2013 sobre a Agência Europeia para a Segurança das Redes e da Informação (**ENISA**) e que revoga o Regulamento (CE) n.º 460/2004 Texto relevante para efeitos do EEE
- 910/2014 sobre serviços de identificação electrónica e de confiança para transacções electrónicas no mercado interno e que revoga a Directiva 1999/93/CE (**eIDAS**[100])
- 679/2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados - **GDPR**)

Decisões do Conselho

- 92/242/CEE no domínio da segurança dos sistemas de informação
- 2005/222/JAI sobre ataques contra os sistemas de informação
- 2011/292/UE sobre as regras de segurança para a protecção da informação classificada da UE

Outros documentos

- Convenção nº 185 do Conselho da Europa sobre Cibercriminalidade
- Protocolo Adicional nº 189 do Conselho da Europa à Convenção sobre a Cibercriminalidade
- Convenção n.º 196 do Conselho da Europa para a Prevenção do Terrorismo
- Regulamento de execução (UE) 2018/151 da Comissão que estabelece as regras de aplicação da Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho no que respeita à especificação dos elementos a ter em conta pelos fornecedores de serviços digitais para a gestão dos riscos colocados à segurança das redes e sistemas de informação e dos parâmetros para determinar se um incidente tem um impacto substancial

Normas internacionais

- Série ISMS ISO/IEC 27000
- na República Checa ČSN ISO/IEC 27001:2014

Actualmente, o documento mais importante da União Europeia relacionado com a questão da ciber-segurança é a DIRECTIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO, de 6 de Julho de 2016, relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação em toda a União Europeia.[101]

Esta directiva está actualmente a ser revista, e a directiva NIS2 está a ser preparada. A primeira lei da UE sobre ciber-segurança, a Directiva NIS, entrou em vigor em 2016 e ajudou a alcançar um nível mais elevado e mais uniforme de segurança das redes e sistemas de informação em toda a UE. Tendo em conta a digitalização sem precedentes dos últimos anos, chegou o momento de a actualizar.

As alterações à directiva revista são devidamente apresentadas no documento da Comissão Europeia[102] :

[100] A seguir referido como o **eIDAS**
[101] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=CS
[102] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72155

NIS	NIS 2
Greater capabilities	
EU Member States improve their cybersecurity capabilities.	More stringent supervision measures and enforcement are introduced. A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established.
Cooperation	
Increased EU-level cooperation.	Establishment of European Cyber crises liaison organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation Group. Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established.
Cybersecurity risk management	
Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.	Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption. Cybersecurity of supply chain for key information and communication technologies will be strengthened. Accountability of the company management for compliance with cybersecurity risk-management measures. Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

SECTORS COVERED BY THE NIS DIRECTIVE

NIS

- HEALTHCARE
- TRANSPORT
- BANKING AND FINANCIAL MARKET INFRASTRUCTURE
- DIGITAL INFRASTRUCTURE
- WATER SUPPLY
- ENERGY
- DIGITAL SERVICE PROVIDERS

4.2 Legislação sobre cibersegurança na República Checa

Em **2000**, o Estado começou a abordar sistematicamente a questão da ciber-segurança.

A Resolução governamental n.º 205 foi adoptada para **tratar de questões de cibersegurança na República Checa** em 2010.[103] Esta resolução estabeleceu o MICR (Ministério do Interior da República Checa) como gestor da questão da ciber-segurança e, ao mesmo tempo, como autoridade nacional para esta área. O Ministro do Interior foi ainda instruído a fazê-lo:

1. coordenar as actividades de outras instituições estatais no domínio da garantia da ciber-segurança,
2. coordenar a representação da República Checa em matéria de cibersegurança em fóruns internacionais, incluindo a participação de organismos estatais nas actividades de organizações internacionais relevantes,
3. submeter o estatuto do Conselho Coordenador Interministerial para a Ciber-Segurança ao governo para aprovação até 30 de Abril de 2010,
4. submeter uma estratégia de ciber-segurança ao governo até 15 de Dezembro de 2010,
5. começar a assegurar o funcionamento do local de trabalho governamental da CSIRT (Equipa de Resposta a Incidentes de Segurança Informática) o mais tardar até 31 de Dezembro de 2010.

Em **19 de Outubro de 2011,** o Governo da República Checa adoptou a Resolução n.º 781 sobre a criação da Autoridade Nacional de Segurança (em checo: Národní bezpečnostní úřad, NBU) como guardiã das questões de ciber-segurança e ao mesmo tempo a autoridade nacional nesta área.[104] Em simultâneo com esta resolução, o Governo da República Checa criou o **Conselho de Segurança**

---

[103] *RESOLUÇÃO DO GOVERNO DA REPÚBLICA CHECA de 15 de Março de 2010 N.º 205 abordando a questão da ciber-segurança da República Checa.* [em linha]. Disponível em: https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ

[104] *RESOLUÇÃO DO GOVERNO DA REPÚBLICA CHECA de 19 de Outubro de 2011 No. 781 sobre a criação da Autoridade Nacional de Segurança como guardiã das questões de cibersegurança e, ao mesmo tempo, da autoridade nacional nesta área.* [em linha]. Disponível em: https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E

Cibernética[105] e aprovou a criação do **Centro Nacional de Segurança Cibernética** (como parte do NBU).

Em **2011,** foi adoptada a **Estratégia para a Ciber-segurança da República Checa para o período de 2011 a 2015**[106] e foi adoptado um **plano de acção para esta estratégia.** Contudo, dada a transferência de responsabilidade do Ministério do Interior para o NBU, esta estratégia é mais frequentemente referida como tal: **Estratégia para a área da cibersegurança da República Checa para o período de 2012 a 2015.**[107]

Os objectivos e medidas estratégicas apresentados foram estabelecidos na estratégia apresentada:

- criação de um quadro legislativo,
- criação do Centro Nacional de Segurança Cibernética e do gabinete governamental CERT,
- protecção de infra-estruturas de informação crítica,
- reforço da ciber-segurança dos sistemas de informação e comunicação da administração pública,
- racionalizar a luta contra a criminalidade no ciberespaço,
- coordenação de actividades para garantir a ciber-segurança na Europa,
- utilização de tecnologias de informação fiáveis e fidedignas,
- sensibilização para a ciber-segurança,
- resposta aos ciberataques.

A 28 de Junho de 2013, o NBU apresentou ao Governo da República Checa um projecto de lei sobre ciber-segurança. O processo legislativo subsequente teve lugar sem quaisquer comentários significativos e a **Lei n.º 181/2014 Coll., sobre Segurança Cibernética e emendas a leis relacionadas** (Lei de Segurança Cibernética) entrou em vigor a 29 de Agosto de 2014 com efeitos a partir de **1 de Janeiro de 2015.**

Em simultâneo com a lei, foram elaborados instrumentos legais estatutários, nomeadamente

- Decreto nº 316/2014, sobre medidas de segurança, incidentes de ciber-segurança, medidas reactivas e sobre a determinação dos requisitos de arquivamento no domínio da ciber-segurança (**Decreto sobre Ciber-segurança**);
- Decreto nº 317/2014, **que estabelece sistemas de informação importantes e os seus critérios de definição**;
- Decreto n.º 315/2014, alteração ao Decreto Governamental n.º 432/2010 Coll., **sobre os critérios para determinar o elemento de infra-estrutura crítica**.

Todos os instrumentos estatutários entraram em vigor ao mesmo tempo que a Lei de Segurança Cibernética.

Em Agosto de 2015, o operador da Equipa Nacional CERT foi seleccionado com base nos requisitos estabelecidos na CSA. A associação CZ.NIC tornou-se este operador.[108] Em 18 de Dezembro de 2015, foi assinado o Contrato Público sobre a Segurança das Actividades da CERT Nacional e sobre a

---

[105] Este conselho é um órgão consultivo do Primeiro Ministro no domínio da ciber-segurança.

[106] *Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015.* [online]. Disponível a partir de: https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura

[107] *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015.* [online]. Disponível em: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieproblastkbnbu.pdf

[108] Ver https://www.nic.cz/page/351/

Cooperação no Domínio da Ciber-segurança.[109] Este contrato foi celebrado por um período indeterminado.

A Lei de Segurança Cibernética sofreu duas alterações significativas desde 2015, ano em que entrou em vigor.

A primeira alteração foi feita pela Lei n.º 104/2017 Coll.,[110] com efeitos a partir de 1 de Julho de 2017 e pela Lei n.º 205/2017 Coll. com efeitos a partir de 1 de Agosto de 2017. Esta alteração alargou o círculo de devedores abrangidos pela CSA para incluir operadores de sistemas de informação e alterou ainda certas sanções.

A segunda alteração significativa de conteúdo foi feita pela Lei n.º 205/2017 Coll.,[111] com efeitos a partir de 1 de Agosto de 2017. Esta alteração implementou a **Directiva 2004/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a assegurar um elevado nível comum de segurança das redes e sistemas de informação na União Europeia (NIS)** na CSA e, ao mesmo tempo, foi criado o **Gabinete Nacional para a Segurança Cibernética e da Informação (NUKIB).** Este assumiu os direitos e obrigações no domínio da ciber-segurança do NBU, incluindo a protecção de informações classificadas nos sistemas de informação e comunicação e a protecção criptográfica. NUKIB é o órgão administrativo central nas áreas acima referidas.

Actualmente, a questão da ciber-segurança é especificamente abordada pela Cybersecurity Act. No entanto, aspectos parciais da protecção da República Checa contra ciberataques podem ser encontrados noutros regulamentos legais. Em termos de ciber-segurança, os documentos mais importantes são os seguintes

Actos constitucionais

- Lei Constitucional n.º 1/1993 Coll., a Constituição da República Checa, com as alterações que lhe foram introduzidas
- Lei Constitucional n.º 2/1993 Coll., Carta dos Direitos e Liberdades Fundamentais, com as alterações que lhe foram introduzidas[112]
- Lei Constitucional n.º 110/1998 Coll., sobre a Segurança da República Checa

Actos

- Lei n.º 106/1999 Coll., sobre o livre acesso à informação, com as alterações que lhe foram introduzidas
- Lei nº 101/2000 Coll., sobre a Protecção de Dados Pessoais e Alteração de Algumas Leis, com as alterações que lhe foram introduzidas[113]

---

[109] Para mais detalhes ver [online]. Disponível a partir de: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf

[110] Lei n.º 104/2017 Coll., que altera a Lei n.º 365/2000 Coll., **sobre Sistemas de Informação da Administração Pública** e que altera algumas outras leis, tal como alterada, Lei n.º 181/2014 Coll., sobre Ciber-segurança e Alteração de Leis Relacionadas (Lei sobre Ciber-segurança) e algumas outras leis. [em linha]. Disponível em: https://www.zakonyprolidi.cz/cs/2017-104

[111] Lei n.º 205/2017 Coll., que altera a Lei n.º 181/2014 Coll., sobre Segurança Cibernética e Leis Relacionadas (Lei sobre Segurança Cibernética), com as alterações que lhe foram introduzidas pela Lei n.º 104/2017 Coll. e por algumas outras leis. [em linha]. Disponível em: https://www.zakonyprolidi.cz/cs/2017-205

[112] A seguir referida como a Carta dos Direitos e Liberdades Fundamentais ou **Carta**.

[113] A seguir referida como a Lei de Protecção de Dados Pessoais ou o **PDPA**. Em relação à eficácia da GDPR, esta lei será rectificada e espera-se que seja substituída pela Lei de Processamento de Dados Pessoais. Para mais pormenores, ver por exemplo [em linha]. Disponível em: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

- Lei nº 121/2000 Coll., sobre Direitos de Autor, sobre Direitos Relacionados com os Direitos de Autor e sobre Alterações a Certas Leis (Copyright Act), com as alterações que lhe foram introduzidas
- Lei nº 240/2000 Coll., sobre gestão de crises e alterações a certas leis (Lei da Crise), com as alterações que lhe foram introduzidas
- Lei n.º 365/2000 Coll., sobre Sistemas de Informação da Administração Pública, com as alterações que lhe foram introduzidas
- Lei n.º 480/2004 Coll., sobre certos serviços da sociedade da informação e sobre alterações a certas leis (Lei sobre certos serviços da sociedade da informação), com as alterações que lhe foram introduzidas [114]
- Lei n.º 127/2005 Coll., sobre Comunicações Electrónicas, com as alterações que lhe foram introduzidas [115]
- Lei n.º 412/2005 Coll., sobre a Protecção de Informações Classificadas e sobre a Autorização de Segurança, com as alterações que lhe foram introduzidas [116]
- Lei n.º 69/2006 Coll., sobre a Imposição de Sanções Internacionais, com as alterações que lhe foram introduzidas
- Lei n.º 300/2008 Coll., sobre Leis Electrónicas e Conversão Autorizada de Documentos, com as alterações que lhe foram introduzidas
- Lei n.º 40/2009 Coll., Código Penal, com as alterações que lhe foram introduzidas [117]
- Lei n.º 111/2009 Coll., sobre Registos Básicos, com as alterações que lhe foram introduzidas
- Lei n.º 418/2011 Coll., relativa à Responsabilidade Penal das Pessoas Colectivas e aos Processos contra elas
- Lei nº 89/2012 Coll., o Código Civil
- **Lei n.º 181/2014 Coll., sobre Ciber-segurança e emendas a leis conexas (Cybersecurity Act)**
- Lei n.º 297/2016 Coll., sobre Serviços Criação de Confiança para Transacções Electrónicas

Instrumentos estatutários

- Decreto Governamental n.º 522/2005 Coll., que estabelece listas de informações classificadas, com as alterações que lhe foram introduzidas
- Decreto nº 523/2005 Coll., sobre a segurança dos sistemas de informação e comunicação e outros dispositivos electrónicos que tratam informações classificadas e sobre a certificação das câmaras de rastreio, com as alterações que lhe foram introduzidas
- Decreto nº 529/2006 Coll., sobre os requisitos de estrutura e conteúdo do conceito de informação e documentação operacional e sobre os requisitos para a gestão da segurança e qualidade dos sistemas de informação da administração pública (Decreto sobre a gestão a longo prazo dos sistemas de informação da administração pública)
- **Regulamento Governamental n.º 432/2010 Coll., sobre os critérios para determinar o elemento de infra-estrutura crítica**

---

[114] A seguir referida como a Lei sobre Certos Serviços da Sociedade da Informação ou **ACISS.**
[115] A seguir referida como **TCE**
[116] A seguir referida como a **PCIA**
[117] A seguir referido como Código Penal ou **CC**.

- Decreto nº 357/2012 Coll., sobre a retenção, transferência e eliminação dos dados de tráfego e localização
- **Decreto nº 317/2014 Coll., sobre sistemas de informação importantes e respectivos critérios de definição**
- **Decreto nº 437/2017 Coll., sobre os critérios para a determinação do operador do serviço de base**
- **Decreto n.º 82/2018 Coll.** , sobre medidas de segurança, incidentes de cibersegurança, medidas reactivas, requisitos de arquivamento no domínio da cibersegurança e eliminação de dados (**Decreto sobre Cibersegurança**)

4.3 Legislação sobre cibersegurança na Polónia

Tendo em conta as circunstâncias legais polacas no domínio da criminalidade informática, deve ser declarado que praticamente todos os crimes incluídos no Capítulo XXXIII do Código Penal podem ser cometidos com a utilização de um computador. Estes tornar-se-ão então crimes informáticos. Em alguns casos, a utilização de um computador constitui uma circunstância que exacerba a responsabilidade criminal, por exemplo, o art. 268 § 2 e 3 do Código Penal, enquanto noutras situações o autor, ao cometer um crime com a utilização de um computador, será tratado da mesma forma que o perpetrador agindo de forma diferente, por exemplo, o art. 265 do Código Penal, art. 266º do Código Penal. Actualmente, como parte do capítulo acima mencionado do Código Penal, o legislador penalizou comportamentos como estes:

- acesso ilegal à informação ou a um sistema informático e com eles relacionado (Artigo 267º do Código Penal)

- actos que consistem em destruir, danificar, remover, substituir informações essenciais ou actividades similares (Artigo 268º do Código Penal),

- acções que consistem em destruir, danificar, apagar, alterar ou obstruir o acesso aos dados informáticos, ou perturbar ou impedir significativamente o processamento, recolha ou transferência automática desses dados (Artigo 268a do Código Penal),

- actos que envolvem a chamada sabotagem informática (Artigo 269º do Código Penal), também conhecida como desvio de TI,

- actos que consistem numa perturbação significativa do funcionamento de um sistema informático ou de uma rede de teleinformação (artigo 269a do Código Penal)

- actos que consistem na produção ilegal (ou actividades similares) de dispositivos ou programas informáticos adaptados para cometer crimes específicos, senhas de computador, códigos de acesso ou outros dados (Artigo 269b do Código Penal).

Para além do capítulo acima mencionado, o legislador regulamentou separadamente o crime de fraude informática (Artigo 287 do Código Penal), o roubo de um programa informático (Artigo 278 § 2 do Código Penal) e o tratamento de um programa informático (Artigo 293 do Código Penal). Todos os delitos incluídos no Capítulo XXXIII pertencem à categoria de delitos comuns, com excepção do Art. 269º do Código Penal, Art. 269a do Código Penal e do art. 269b do Código Penal. São de natureza de aplicação.

As soluções adoptadas no Capítulo XXXIII do Código Penal são uma consequência da assinatura pela Polónia, a 23 de Novembro de 2001, da Convenção n.º 185 do Conselho da Europa sobre o Cibercrime e da Decisão-Quadro 2005/222 / JAI do Conselho relativa a ataques contra os sistemas de informação.

O artigo 267º do Código Penal constitui a protecção penal da privacidade dos utilizadores da Internet. Em arte. 267 § 1 do Código Penal penaliza as acções destinadas a obter o acesso ilegal a informações não destinadas ao autor do crime. Do ponto de vista do registo criminal do comportamento do perpetrador, não importa onde a informação é armazenada, seja no disco rígido ou num servidor externo da rede. Isto significa que esta disposição protege o direito subjectivo amplamente compreendido de dispor de informações. A conduta do perpetrador da ofensa especificada na arte. 267 § 1 do Código Penal pode consistir na abertura de uma carta fechada, na ligação a uma rede de telecomunicações ou na quebra ou ultrapassagem de medidas electrónicas, magnéticas, informáticas ou outras medidas especiais de segurança. O conteúdo da disposição indica que o legislador penaliza as actividades indicadas na parte dispositiva, independentemente de o autor da infracção ter lido o conteúdo da informação. Isto significa que as características de um crime ao abrigo do art. 267 do Código Penal serão também preenchidas por uma pessoa que terá acesso a informações que não lhe sejam destinadas, mesmo numa situação em que não tenha a intenção de ler o seu conteúdo. A privacidade dos utilizadores da Internet também pode ser violada, quebrando ou contornando as medidas de segurança existentes e, assim, invadindo o computador da vítima. O termo genérico em Arte. 267 § 1 do Código Penal tipos de segurança, cuja violação ou desvio é punível por lei, significa que a securização de um ficheiro com uma palavra-passe irá satisfazer as condições de informação securizada.

As acções do perpetrador destinadas a obter acesso a todo ou parte do sistema informático constituem uma ofensa ao abrigo da Arte. 267 § 2 do Código Penal Referindo-se ao objecto do acto, chama-se a atenção para o termo "rede de telecomunicações" utilizado pelo legislador, que não foi definido no Código Penal. Por conseguinte, parece necessário referir-se ao art. 2 pontos 35 da Lei de 16 de Julho de 2004 das Telecomunicações, que define a rede de telecomunicações como sistemas de transmissão e dispositivos de comutação ou redireccionamento, bem como outros recursos, incluindo elementos inactivos da rede que permitem a transmissão, recepção ou transmissão de sinais através de fios, ondas de rádio, meios ópticos ou outros, utilizando energia electromagnética, qualquer que seja o seu tipo. A análise da definição acima mostra que uma rede de telecomunicações pode ser tanto a infra-estrutura de cabo existente como uma rede sem fios.

Além disso, o conceito de um sistema informático não foi definido no Código Penal, a sua definição é dada no Art. 7 ponto 2a da Lei de 29 de Agosto de 1997 sobre a Protecção de Dados Pessoais, que estabelece que "um sistema informático é um conjunto de dispositivos, programas, procedimentos de processamento de informação e ferramentas informáticas utilizadas para processar dados que cooperam entre si". Este termo também aparece no Art. 1 lit. e na Decisão-Quadro 2005/222 / JAI do Conselho de 24 de Fevereiro de 2005, que especifica que um sistema informático é qualquer dispositivo ou grupo de dispositivos ligados ou relacionados, dos quais pelo menos um efectua o tratamento automático de dados informáticos em conformidade com o software, bem como os dados armazenados, processados, recuperados ou fornecidos pelos mesmos para efeitos do seu funcionamento, utilização, protecção ou manutenção. Uma outra definição de um sistema informático está contida na Convenção n.º 185 do Conselho da Europa sobre Cibercriminalidade. Nos termos do artigo. 1 lit. e da Convenção, um sistema de informação é qualquer dispositivo ou grupo de dispositivos interligados ou relacionados, um ou mais dos quais, de acordo com o programa, efectua o processamento automático de dados. Devido ao facto de o conceito de um sistema informático desempenhar um papel importante na determinação da responsabilidade pelo cibercrime, a literatura descreve um sistema informático como um conjunto de elementos de hardware e software de cooperação que são utilizados para introduzir, processar e ler informação. O sistema informático não inclui, portanto, instalações de transmissão de dados.

Vale a pena notar que o legislador em Arte. 267 § 2 do Código Penal não definiu o método da acção do perpetrador, mas apenas o seu efeito. O acima exposto exige que qualquer comportamento que consista no acesso não autorizado a um sistema informático seja penalizado, independentemente de ter havido qualquer violação da segurança do computador ou do sistema.

Em arte. 267 § 3 do Código Penal, o legislador sanciona outro acto proibido que consiste em instalar ou utilizar um dispositivo de escuta, um dispositivo visual ou outro dispositivo ou software, a fim de obter informações a que não tem direito. A condição de responsabilidade nos termos desta disposição não é a obtenção de informações, é suficiente que o infractor tome medidas específicas. Contudo, estas acções devem ser tomadas para um fim específico, ou seja, para obter informações a que o perpetrador não tem direito.

Em arte. 267 § 4 do Código Penal, o legislador penaliza a divulgação de informações obtidas a outra pessoa da forma especificada nos § 1-3.

Outra arte. 268 do Código Penal sanciona o comportamento do perpetrador com o objectivo de violar a integridade dos dados informáticos. De acordo com as disposições do acto, esta violação pode tomar a forma de destruir, danificar, apagar ou alterar o registo de informações essenciais.

Em arte. 268 § 2 do Código Penal O legislador cobriu a situação quando o acto do perpetrador diz respeito à gravação num suporte de dados TI, por exemplo, um disco rígido ou um CD. Note-se que o tema da protecção da Arte. 268 do Código Penal é a disponibilidade de informações, e o objectivo da acção do perpetrador é impedir ou impedir significativamente o acesso às informações relevantes por parte da pessoa autorizada. A necessidade da ocorrência de um efeito sob a forma de frustração ou de impedimento significativo do acesso à informação significa que um delito que consiste em destruir, danificar, apagar, substituir informações essenciais ou actividades similares se enquadra na categoria de delitos consequentes. Tal qualificação é consistente com a visão bem estabelecida da literatura. O legislador em Arte. 268 do Código Penal utiliza o conceito de "informação material" sem indicar as características que a informação deve ter para ser material, na acepção desta disposição. Por conseguinte, a avaliação da natureza das informações em questão deve ser feita caso a caso, com base em critérios objectivos e subjectivos.

O tema da protecção da arte. 268a do Código Penal, em oposição à Arte. 268 do Código Penal, foi amplamente definido e é a segurança e disponibilidade dos dados informáticos, que não têm de satisfazer as características de significância. Os sinais de uma ofensa ao abrigo do art. 268a do Código Penal estão a destruir, danificar, apagar, alterar ou obstruir o acesso aos dados informáticos. Penalizados na arte. 268a do Código Penal o comportamento também pode consistir em perturbar ou impedir significativamente o processamento, recolha ou transferência automática de dados informáticos. O segundo conjunto de comportamentos proibidos deve ser significativo, que deve estar relacionado com o grau de perturbação ou prevenção do tratamento, recolha ou transmissão automática de dados informáticos, e não com a extensão dos dados modificados pelo perpetrador. Falamos da importância das acções tomadas pelo perpetrador quando estas acções são caracterizadas por um grau de intensidade suficientemente elevado. O tema da protecção da arte. 268a do Código Penal é a segurança da informação armazenada, transmitida e processada em sistemas baseados em dados TI.

Com base no sistema jurídico polaco, o termo "dados informáticos" não foi definido, e desempenha um papel importante. Por conseguinte, é necessário fazer referência ao direito internacional - em conformidade com o conteúdo da Arte. 1 letra b da Convenção n.º 185 do Conselho da Europa sobre o Cibercrime. De acordo com a disposição citada, este termo significa "qualquer representação de factos, informações ou conceitos de uma forma adequada ao processamento num sistema informático, incluindo um programa apropriado causando o desempenho de uma função por um sistema informático".

A definição de dados informáticos está também incluída na Arte. 1 letra b da Decisão-Quadro 2005/222 / JAI do Conselho de 24/02/2005 sobre ataques contra sistemas de informação e significa "qualquer representação de factos, informações ou ideias numa forma adequada ao processamento num sistema de informação, incluindo um programa adequado para causar o desempenho de uma função pelo sistema".

As definições apresentadas indicam que os dados informáticos são todos os dados que são portadores de informação, bem como os programas informáticos utilizados tanto por pessoas individualmente definidas como utilizados em redes de TIC por um número indefinido de pessoas.

Em arte. 269 do Código Penal, o legislador penalizou o comportamento da chamada sabotagem informática. A essência deste crime é a destruição, dano, eliminação ou alteração de dados informáticos de particular importância para a defesa do país, segurança nas comunicações, funcionamento da administração governamental, outro órgão ou instituição estatal ou governo local, bem como a perturbação ou impedimento do processamento, recolha ou transferência automática desses dados.

Em arte. 269 § 2 do Código Penal, o legislador indicou que o crime de sabotagem pode consistir na destruição ou substituição de um portador de dados TI ou na destruição ou danificação de um dispositivo utilizado para o processamento, recolha ou transmissão automática de dados TI. Como decorre do conteúdo da disposição em questão, os dados TI são objecto de protecção de particular importância para a defesa do país, segurança nas comunicações, funcionamento da administração governamental, outro organismo estatal ou administração local, e o sistema de tratamento, recolha ou transferência automática de tais informações. A sabotagem informática é considerada como um tipo qualificado em relação aos crimes previstos na Arte. 268 § 2 do Código Penal, Art. 268a do Código Penal e 269a do Código Penal. A marca de qualificação aqui é o tipo de dados protegidos, ou seja, dados de particular importância para os valores enumerados no art. 268º do Código Penal. 269 do Código Penal. O legislador dividiu o comportamento penalizado do perpetrador em dois grupos. O primeiro deles são actividades destinadas a destruir, danificar, apagar ou alterar dados informáticos de particular importância para os valores protegidos pelo regulamento. O tema da protecção desta parte da disposição é a integridade dos dados pertencentes a uma categoria específica. O segundo grupo de características são actividades que consistem em perturbar ou impedir o tratamento, recolha ou transferência automática de dados informáticos de particular importância para a defesa do país, segurança nas comunicações, funcionamento da administração governamental, outro organismo ou instituição estatal ou governo local. Neste caso, o objecto de protecção é a disponibilidade dos dados especificados na disposição supracitada.

Em arte. 269 § 2 do Código Penal, o legislador, protegendo os bens especificados no § 1, sancionou os actos do autor do crime que consistiam em destruir ou substituir um portador de dados TI ou destruir ou danificar dispositivos utilizados para o processamento, recolha ou transmissão automática de dados TI. Estas actividades podem consistir na destruição física, danos, substituição de, por exemplo, discos rígidos, bem como em dificultar ou impedir o seu processamento, por exemplo, danificando dispositivos de rede. Devido à natureza material do crime de sabotagem informática, por atribuir ao perpetrador um acto ao abrigo da Arte. 269 do Código Penal, é necessário ter um efeito específico sob a forma de destruição ou dano dos dados informáticos especificados ou perturbar ou impedir o seu processamento ou transmissão automáticos.

Outra disposição que regula a responsabilidade criminal da cibercriminalidade é a Arte. 269a do Código Penal polaco. A essência desta disposição é a protecção da segurança operacional de um sistema informático ou de uma rede TIC. O conceito de um sistema informático é identificado na literatura com o conceito de um sistema de informação. A responsabilidade criminal ao abrigo desta disposição será imposta a uma pessoa que, sem o direito, interfira significativamente com o funcionamento de um sistema informático ou rede de teleinformação por transmissão, destruição, remoção, dano, obstrução de acesso ou alteração de dados informáticos. Os métodos de acção penalizados pelo acto foram enumerados na disposição e, como regra, não devem suscitar quaisquer dúvidas de interpretação. A excepção é o termo "transmissão", que não foi definido pelo legislador. Na literatura, este termo significa a transferência de informação de um local num sistema informático para outro, por exemplo, de memória operacional para disco, de disco para impressora, de um computador numa rede para outro computador em rede. A transmissão sancionada de dados informáticos à distância deve ter lugar de forma codificada, e não em suportes externos, como um CD.

O artigo 269b do Código Penal sanciona a produção, aquisição, venda ou disponibilização a outras pessoas de dispositivos ou programas informáticos adaptados para cometer os crimes enumerados. É de notar que as características deste crime incluem uma série de actividades preparatórias que podem estar relacionadas com a prática de crimes indicados na parte dispositiva da disposição. A criminalização abrange as actividades que consistem na criação e adaptação de dispositivos ou programas para a prática de crimes ao abrigo do art. 165 § 1 ponto 4, art. 267 § 3, art. 268a § 1 ou § 2 em relação ao § 1, art. 269 § 2, art. 269 § 2, ou artigo. 269a, a sua partilha e obtenção, bem como a quebra de senhas de computador, códigos de acesso ou outros dados que permitam o acesso à informação armazenada num sistema informático ou numa rede de TIC. O tema da protecção é a segurança da informação processada electronicamente em todos os aspectos, ou seja, a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos. Embora o legislador utilize o plural para actividades sancionadas, um único comportamento, por exemplo, a venda de apenas um programa, será punido por lei. Tal ponto de vista é estabelecido tanto na doutrina como na jurisprudência.

Em arte. 287 do Código Penal, o legislador regulamentou o crime de fraude informática. Esta infracção está incluída no capítulo XXXV, "Infracções contra a propriedade". O objecto de protecção deste artigo são os dados informáticos, juntamente com as informações nele contidas. Estes dados podem ser armazenados tanto na memória do computador como num CD ou servidor. O comportamento penalizado do infractor consiste em influenciar sem autorização o processamento, recolha ou transmissão automática de informações ou a alteração, eliminação ou introdução de um novo registo nos dados informáticos. O comportamento descrito do perpetrador deve ter como objectivo obter ganhos financeiros ou causar danos a outra pessoa. A literatura indica que a acção do perpetrador destinada a influenciar o processamento, recolha ou transmissão automática de informações assume a forma de interferência ilegal por parte de uma entidade externa no decurso de processos automáticos, o que faz com que, após a influência do perpetrador terminar o seu curso, em particular o processamento, recolha ou transmissão, seja diferente do que se o acto do perpetrador não tivesse sido executado. A fraude informática é um delito criminal. Isto significa que a infracção ao abrigo da Arte. 287 § 1 do Código Penal é feita no momento da introdução de alterações ou outras interferências no dispositivo ou sistema de recolha, processamento ou transmissão de informações através de tecnologia informática, tal como descrito nesta disposição. A necessidade do dano não é uma das suas marcas distintivas.

Em arte. 287 § 2 do Código Penal, o legislador definiu o tipo privilegiado devido a um caso menor. A ofensa ao abrigo do art. 287º do Código Penal, tem, por regra, carácter de Ministério Público. Contudo, no caso de ter sido cometido em detrimento da pessoa mais próxima, provoca, de acordo com o disposto no § 3, a alteração do modo de acção penal para o pedido.

A análise acima referida das disposições que regulam a responsabilidade criminal em matéria de crimes informáticos indica que o objecto fundamental de protecção para a criminalização dos crimes informáticos é a tradicional liberdade e privacidade dos indivíduos, embora visto de uma perspectiva informática. Contudo, também os dados recolhidos nos sistemas são protegidos, bem como os próprios sistemas e a sua integridade, cuja violação pode frequentemente ter consequências sociais muito graves. Ao mesmo tempo, deve ser mencionado que a regulamentação penal da cibercriminalidade irá encontrar dois problemas fundamentais. O primeiro está relacionado com o princípio da jurisdição. A criminalidade informática cometida na Internet é muitas vezes de natureza transfronteiriça, e por vezes até territorial, no sentido em que é frequentemente cometida isoladamente do território de uma determinada jurisdição. O segundo problema é o desenvolvimento muito rápido de novas formas de cibercriminalidade, que os legisladores normalmente não acompanham.

No entanto, tendo em conta os aspectos de direito penal apresentados, a gravidade da ameaça representada pelo cibercrime e a necessidade de uma resposta adequada ao mesmo, em particular através de regulamentos no domínio do direito penal, não pode levantar quaisquer dúvidas.

4.4 Legislação sobre cibersegurança em Portugal

Conserte-me

5. Sistema de Gestão da Segurança da Informação

5.1 Estrutura do SGSI

O **Information Security Management System** (**ISMS**)[118] **é um conjunto de regras** concebidas para manter a confidencialidade, integridade e disponibilidade da informação, aplicando um processo de gestão de riscos e dando garantias às partes interessadas de que os riscos estão a ser geridos adequadamente. [119]

No âmbito do SGSI, os bens são protegidos, os riscos de segurança da informação são geridos e as medidas já em vigor são verificadas.

Sistema de gestão da segurança da informação significa uma parte do sistema de gestão que se baseia na abordagem dos riscos do sistema de informação e comunicação. Esta parte do sistema de gestão define como estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação e dos dados.

É também claro, pela definição acima referida, que o **SGSI faz parte dos processos e do sistema global de gestão de uma organização, além de estar integrado nestes sistemas.**

O SGSI pode ser aplicado a uma organização como um todo, bem como a uma unidade organizacional dentro da organização, ou a um sistema de informação e comunicação especificamente concebido, ou parte dele.

"O SGSI pode ser implementado e utilizado numa organização com dez empregados, bem como numa grande empresa holding que pode ter milhares de empregados. Em termos simples, existe apenas um SGSI, o descrito na norma ISO/IEC 27001. Contudo, a interpretação e implementação de recomendações individuais podem variar significativamente dependendo do âmbito do sistema, do número de utilizadores, da forma como os dados são processados, do seu valor e especialmente de acordo com os riscos reais de segurança, etc. A estratégia do SGSI em pequenas e médias empresas não é descrita com tanto detalhe como é habitual em grandes organizações, especialmente multinacionais.

O SGSI não se aplica apenas a empresas industriais e organizações privadas, o SGSI aplica-se a todas as organizações, incluindo instituições de direito público e organismos estatais. Isto é demonstrado pela existência de muitas resoluções governamentais e departamentais nacionais que

[118] A seguir referido como o **SGSI**
[119] Cf. introdução ISO/IEC 27001

recomendam ou exigem a implementação do SGSI em organizações geridas e estabelecidas pelo Estado".[120]

Muitas normas ISMS são concebidas para ajudar organizações de todos os tipos e tamanhos a implementar e operar o ISMS. Consistem nas seguintes normas internacionais, colectivamente referidas como (*Tecnologia da Informação - Tecnologias de Segurança*[121] (listadas abaixo em ordem numérica):

- ISO/CEI 27000 — *Sistemas de gestão da segurança da informação - Visão geral e vocabulário*
- **ISO/IEC 27001** — ***Sistemas de Gestão de Segurança da Informação - Requisitos***
- ISO/IEC 27002 — *Código de prática para controlos de segurança da informação*
- ISO/IEC 27003 — *Sistemas de gestão da segurança da informação - Orientação*
- ISO/IEC 27004 — *Gestão da segurança da informação - Monitorização, medição, análise e avaliação*
- ISO/IEC 27005 — *Gestão do risco de segurança da informação*
- ISO/IEC 27006 — *Requisitos para os organismos de auditoria e certificação dos sistemas de gestão da segurança da informação*
- ISO/IEC 27007 — *Directrizes para a auditoria de sistemas de gestão de segurança da informação*
- ISO/IEC TR 27008 — *Directrizes para auditores sobre controlos de segurança da informação*
- ISO/IEC 27009 — *Aplicação sectorial específica da ISO/IEC 27001 - Requisitos*
- ISO/IEC 27010 — *Gestão da segurança da informação para comunicações inter-sectoriais e inter-organizacionais*
- ISO/IEC 27011 — *Código de prática para controlos de segurança da informação baseado na ISO/IEC 27002 para organizações de telecomunicações*
- ISO/CEI 27013 — *Orientações sobre a implementação integrada da ISO/CEI 27001 e ISO/CEI 20000-1*
- ISO/IEC 27014 — *Governação da segurança da informação*
- ISO/IEC TR 27015 — *Directrizes de gestão da segurança da informação para serviços financeiros*

---

[120] PO`ÁR, Josef e Luděk NOVÁK. *Pracovní příručka bezpečnostního manaizera.* Praga: AFCEA, 2011. ISBN 978-80-7251-364-2, p. 5, ou: PO`ÁR, Josef e Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Disponível em: https://www.cybersecurity.cz/data/srib.pdf p. 1

[121] O nome comum *"Tecnologia da Informação - Técnicas de Segurança"* indica que estas normas internacionais foram preparadas pelo comité técnico conjunto ISO/IEC JTC 1 *Tecnologias da Informação*, subcomité SC 27 *IT Security Techniques*

- ISO/IEC TR 27016 — *Gestão da segurança da informação - Economia organizacional*
- ISO/CEI 27017 — *Código de prática para controlos de segurança da informação baseado na ISO/IEC 27002 para serviços em nuvem*
- ISO/CEI 27018 — *Código de prática para protecção de informações pessoalmente identificáveis (IPI) em nuvens públicas que actuam como processadores de IPI*
- ISO/CEI 27019 — *Orientações de gestão da segurança da informação baseadas na ISO/IEC 27002 para sistemas de controlo de processos específicos para a indústria de serviços públicos de energia*

As normas internacionais, que não estão listadas sob este nome comum mas que também fazem parte de uma série de normas ISMS, estão listadas abaixo:

- ISO 27799 — *Informática da saúde - Gestão da segurança da informação na saúde utilizando a ISO/IEC 27002*[122]

A solução ISMS requer uma abordagem sistémica e abrangente, respeitando os princípios e elementos de todo o ciclo de vida da ciber-segurança. O sistema de gestão do SGSI baseia-se no ciclo de Deming, ou também no **ciclo PDCA** (Plan-Do-Check-Act).

O ciclo PDCA é um dos princípios básicos de gestão baseado na melhoria gradual da qualidade dos processos, serviços, dados, produtos, etc., graças à repetição constante das suas quatro actividades básicas: Plan-Do-Check-Act.

Existem actualmente várias variantes do ciclo PDCA[123] , e uma das modificações adequadas deste ciclo, que também é aplicável no campo da ciber-segurança, é a variante **OPDCA**, que estende o modelo original pela fase **Observar que precede** a fase do Plano.

O ciclo PDCA, ou algumas das suas modificações, pode ser aplicado a todos os processos do SGSI. A forma mais simples de exibir este modelo é um círculo interminável:

Figura: Modelo PDCA[124]

O modelo PDCA também foi expresso na ISO/IEC 27001: 2005 e ilustrou como o SGSI aceita os requisitos de segurança da informação e as expectativas das partes interessadas como um input e utiliza a informação e os processos para gerar resultados de segurança da informação que satisfaçam esses requisitos e expectativas.

[122] Para uma visão geral das normas, ver: ČSN PT ISO/IEC 27000 (369790) - Tecnologias da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Visão geral e vocabulário

[123] ROSER, Christoph. *The Many Flavors of the PDCA.* [em linha]. [cit. 06/07/2018]. Disponível em: https://www.allaboutlean.com/pdca-variants/

[124] *Ciclo PDCA.* [online]. [cit. 06/07/2018]. Disponível em: https://www.creativesafetysupply.com/glossary/pdca-cycle/

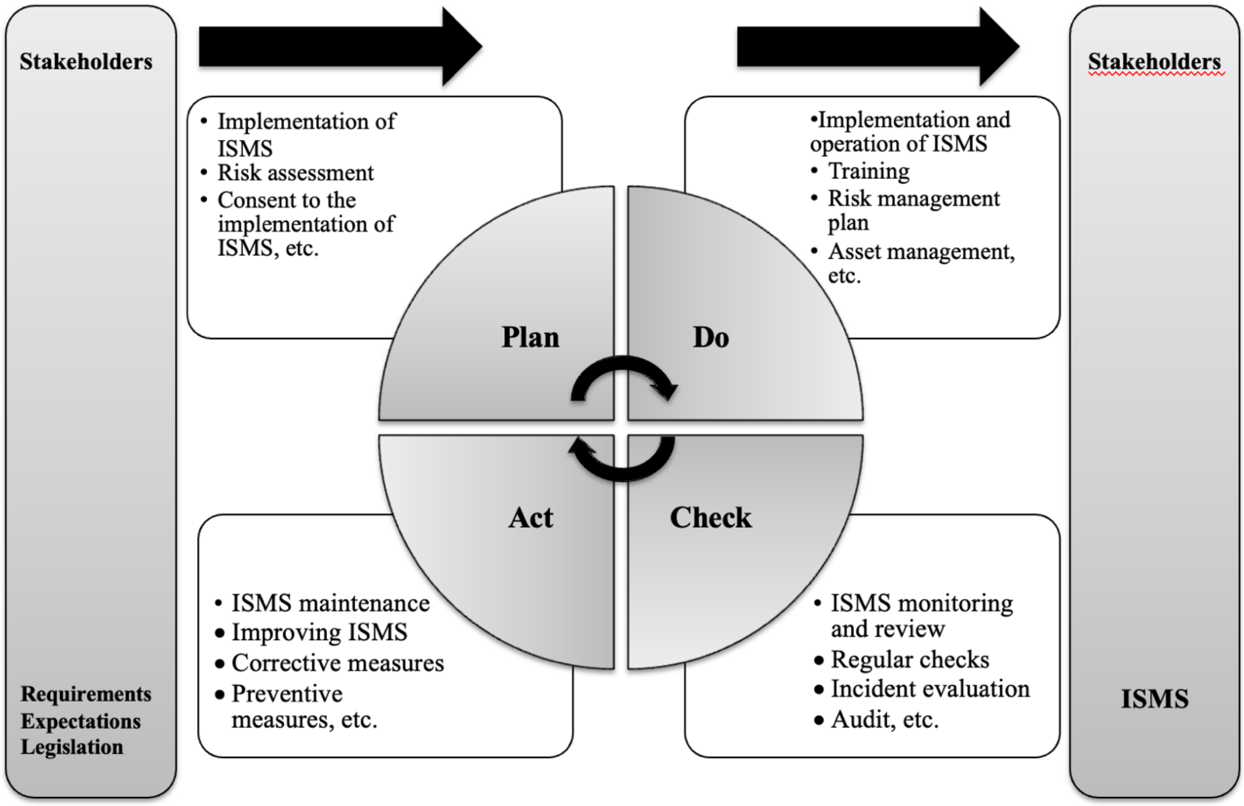


Figura: Modelo PDCA aplicado aos processos ISMS[125]

Plano (estabelecimento do ISMS)	Estabelecimento da política, objectivos, processos e procedimentos do SGSI relacionados com a gestão de riscos e segurança da informação para fornecer resultados consistentes com a política e objectivos globais da organização.
Fazer (implementação e funcionamento do SGSI)	Implementação e utilização da política, medidas, processos e procedimentos do SGSI.
Verificação (monitorização e revisão do SGSI)	Avaliar, sempre que possível, a medição do desempenho do processo face à política, objectivos e experiência prática do SGSI e comunicar os resultados à direcção da organização para análise.
Actuar (manter e melhorar o ISMS)	Tomar medidas correctivas e preventivas com base nos resultados da auditoria interna do SGSI e revisão do sistema de gestão pela direcção da organização para assegurar a melhoria contínua do SGSI.

A norma ISO/IEC 27001 promove a adopção de uma abordagem de processo para **estabelecer, implementar, operar, monitorizar, manter e melhorar o SGSI** numa organização. A tónica é colocada especialmente:

- compreensão dos requisitos de segurança da informação de uma organização e da necessidade

[125] Modelo PDCA modificado e complementado. O modelo original foi introduzido na norma ISO/IEC 27001: 2005 p. 7

de definir políticas e objectivos de segurança da informação,

- introdução e funcionamento de medidas para a gestão da segurança da informação no contexto da gestão dos riscos globais das actividades de uma organização,
- monitorização e revisão do desempenho e eficiência do SGSI,
- melhoria contínua com base em medições objectivas.

"Para o SGSI dentro de uma organização, a organização de gestão, a responsabilidade pela segurança da informação dos gestores a todos os níveis, organismos profissionais e papéis no sistema de segurança da informação deve ser claramente descrita.

Na estrutura organizacional de uma organização, a segurança da informação deve ser tida em conta de modo a abranger as actividades e cooperação da direcção, pessoas responsáveis pelos sistemas de aplicação, serviços operacionais, utilizadores finais e pessoas responsáveis por actividades individuais. A segurança da informação pressupõe a estreita cooperação de todos os grupos de empregados mencionados e a prestação de formação no domínio da segurança da informação, para que, para além dos responsáveis pela segurança da informação e de outros elementos da organização, o pessoal de gestão da informação e todos os utilizadores da tecnologia da informação tenham também um conhecimento básico da segurança da informação".[126]

Em relação ao acima exposto, é possível definir objectivos padrão do SGSI dentro de uma organização:

- garantir a segurança dos sistemas e serviços de informação e comunicação,
- assegurar a continuidade do funcionamento dos sistemas e serviços de informação e comunicação,
- protecção de dados e informações,
- protecção de outros bens,
- tratamento de ameaças, eventos e incidentes, incluindo a prevenção,
- aumentar a segurança dos sistemas e serviços de informação e comunicação,
- a sensibilização geral dos utilizadores sobre segurança e ameaças à segurança (educação),
- partilha de experiências com outras entidades.

No entanto, a **implementação do SGSI** numa organização **não pode garantir a segurança completa dos bens da organização.** Contudo, a implementação do SGSI pode reduzir significativamente os riscos de invasão de activos a um nível aceitável. Todo o sistema é tão forte como o seu elo mais fraco. Neste caso, o elo mais fraco, e o maior perigo para a segurança da informação, é uma pessoa.

5.2 Gestão do risco

Nos termos do artigo 7º do SRI, cada Estado-Membro deve adoptar uma estratégia nacional de segurança das redes e sistemas de informação, definindo objectivos estratégicos e medidas políticas e regulamentares relevantes para alcançar e manter um elevado nível de segurança das redes e sistemas de informação. O tema da estratégia nacional para a segurança das redes e dos sistemas de informação inclui principalmente os seguintes objectivos e medidas:

[126] PO`ÁR, Josef e Luděk NOVÁK. *Pracovní příručka bezpečnostního manaizera.* Praga: AFCEA, 2011. ISBN 978-80-7251-364-2, pp. 7-8, ou: PO`ÁR, Josef e Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Disponível em: https://www.cybersecurity.cz/data/srib.pdf p. 2

a) os objectivos e prioridades da estratégia nacional para a segurança das redes e da informação;

b) o quadro administrativo para cumprir os objectivos e prioridades da estratégia nacional para a segurança das redes e sistemas de informação, incluindo o papel e as responsabilidades dos governos e outras entidades relevantes;

c) identificação de medidas de preparação, resposta e recuperação, incluindo cooperação entre os sectores público e privado;

d) definição de programas de educação, informação e formação relacionados com a estratégia nacional para a segurança das redes e dos sistemas de informação;

e) definição de planos de investigação e desenvolvimento relacionados com a estratégia nacional de segurança de redes e sistemas de informação;

f) plano de avaliação de risco para identificação de riscos;

g) uma lista das várias entidades envolvidas na implementação da estratégia nacional para a segurança das redes e dos sistemas de informação.

De acordo com a legislação checa, a **avaliação de risco** significa o **processo global de identificação, análise e avaliação do risco.**

O processo de avaliação de risco é abordado, por exemplo, pela ISO/IEC 27005, onde este processo é demonstrado.

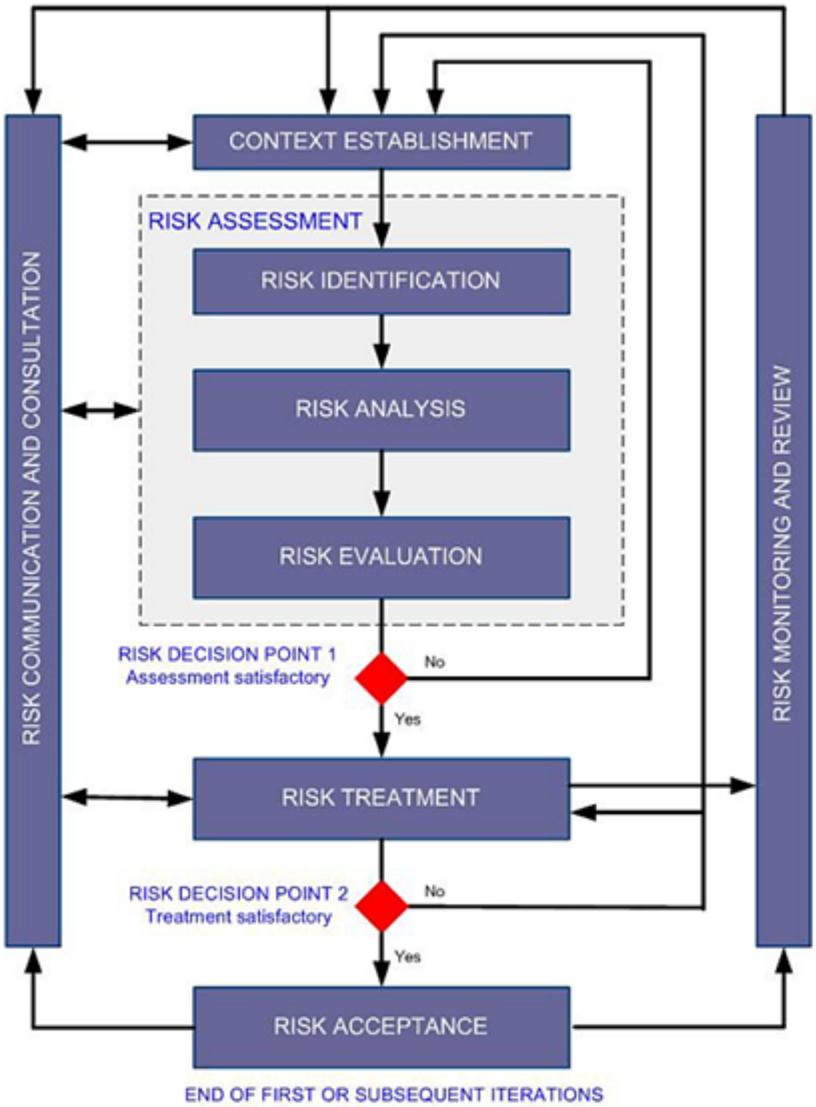


Figura: Demonstração da avaliação dos riscos no SGSI[127]

O modelo PDCA também deve ser respeitado no processo de avaliação de risco, mas é adaptado para a avaliação de risco.[128]

Processo ISMS	**Processo de avaliação de risco no SGSI**
Plano	Criação de um contexto Avaliação de risco Desenvolvimento de um plano de gestão de risco Aceitação de riscos
Faça	Implementação do plano de gestão do risco
Verifique	Acompanhamento contínuo e revisão dos riscos
Lei	Manter e melhorar o processo de avaliação e gestão dos riscos

[127] ISO/IEC 27005 p. 8
[128] ISO/IEC 27005 p. 9

	Processo de gestão

Quanto à gestão do risco em si, é possível ilustrar graficamente este processo da seguinte forma:

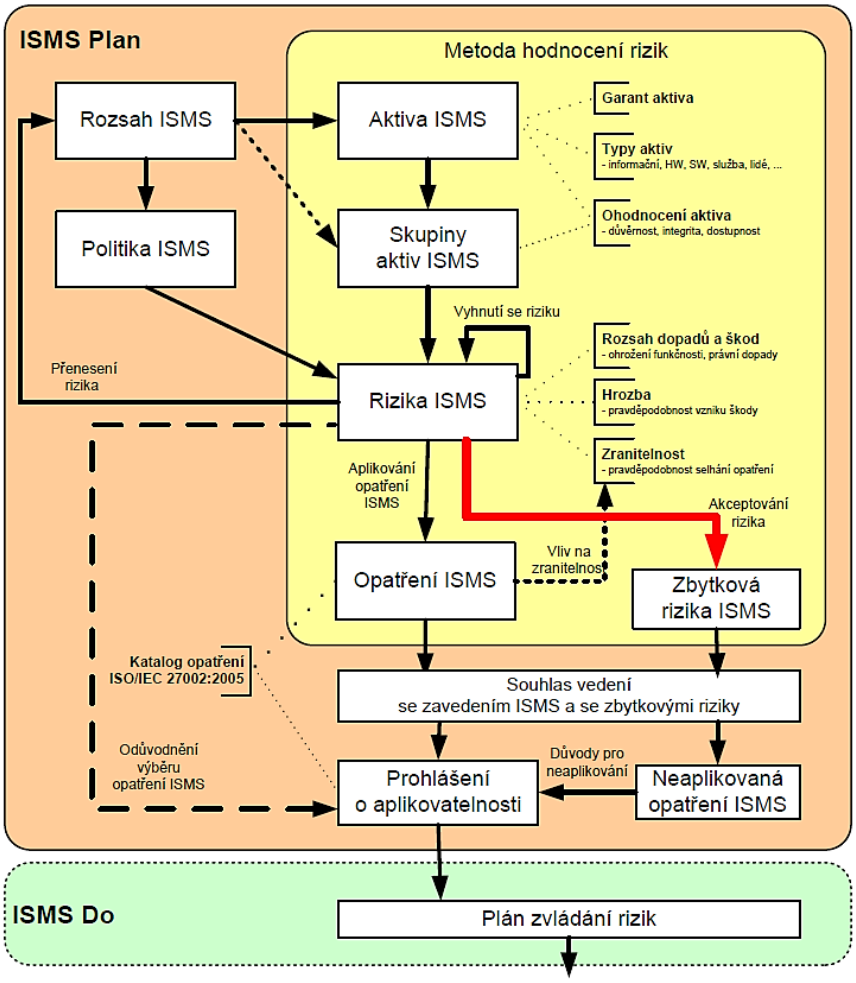


Figura: Gestão de risco no processo do SGSI[129]

Plano ISMS	**Plano ISMS**
Rozsah ISMS	Âmbito do SGSI
Politika ISMS	Política do SGSI
Přenesení rizika	Transferência de risco
Katalog opatření ISO/IEC 27002:2005	Catálogo de medidas ISO/IEC 27002:2005
Odůvodnění výběru opatření ISMS	Justificação para a escolha de medidas ISMS
Souhlas vedení se zavedením ISMS a se zbytkovými riziky	Aprovação da gestão da implementação do SGSI e riscos residuais
Prohlášení a aplikovatelnosti	Declaração e aplicabilidade
Důvody pro neaplikování	Razões para não se aplicar
Neaplikovaná opatření ISMS	Medidas ISMS não aplicadas
Metoda hodnocení rizik	Método de avaliação de risco
Aktiva ISMS	Activos do SGSI
Garant aktiva	Fiador de bens
Typy aktiv - informační, HW, SW, sluzba, lidé, ...	Tipos de bens - informação, HW, SW, serviço, pessoas, ...

[129] PO`ÁR, Josef e Luděk NOVÁK. *Pracovní příručka bezpečnostního manaizera.* Praga: AFCEA, 2011. ISBN 978-80-7251-364-2, p. 12, ou: PO`ÁR, Josef e Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Disponível em: https://www.cybersecurity.cz/data/srib.pdf p. 5

Ohodnocení aktiva - důvěrnost, integrita, dostupnost	Avaliação de activos - confidencialidade, integridade, disponibilidade
Skupiny aktiv ISMS	Grupos de activos do SGSI
Vyhnutí se riziku	Evitar riscos
Rozsah dopadů a škod - ohrození funkčnosti, právní dopady	Extensão dos impactos e danos - perigo de funcionalidade, consequências legais
Hrozba - pravděpodobnost vzniku škody	Ameaça - probabilidade de danos
Zranitelnost - pravděpodobnost selhání opatření	Vulnerabilidade - probabilidade de falha de uma medida
Rizika ISMS	Riscos do SGSI
Aplikování opatření ISMS	Aplicação das medidas do SGSI
Akceptování rizika	Aceitação de riscos
Opatření ISMS	Medidas do SGSI
Vliv na zranitelnost	Impacto na vulnerabilidade
Zbytková rizika ISMS	Riscos residuais do SGSI
O ISMS faz	**O ISMS faz**
Plán zvládání rizik	Plano de gestão de risco

O valor do risco é mais frequentemente expresso como uma função afectada pelo impacto, ameaça e vulnerabilidade. Por exemplo, a seguinte função pode ser utilizada para a auto-avaliação do risco:

Risco = impacto * ameaça * vulnerabilidade

Se um devedor utilizar um método de avaliação de risco que não faça distinção entre avaliações de ameaça e de vulnerabilidade, as escalas de avaliação de ameaça e de vulnerabilidade podem ser combinadas. A fusão das escalas não deve levar a uma perda da capacidade de distinguir entre níveis de ameaça e vulnerabilidade. Para este fim, por exemplo, pode ser utilizado um comentário que expresse claramente tanto o nível de ameaça como o nível de vulnerabilidade. O mesmo se aplica nos casos em que o devedor utiliza um número diferente de níveis para avaliar impactos, ameaças, vulnerabilidades e riscos.[130]

O apêndice 3 do CSD enumera ainda as escalas utilizadas para avaliar ameaças, vulnerabilidades e riscos.

Nível	**Descrição**
Baixo	A ameaça não existe ou é improvável. A tentativa de ameaça esperada **não** é **mais frequente do que uma vez a cada 5 anos**.
Médio	É pouco provável que a ameaça seja provável. A tentativa de ameaça esperada situa-se no intervalo de **1 ano a 5 anos**.
Alto	É provável que a ameaça seja muito provável. A tentativa de ameaça esperada situa-se no intervalo de **1 mês a 1 ano**.
Crítico	Ameaça é muito provável ou mais ou menos certa. A tentativa de ameaça esperada **é mais frequente do que uma vez por mês**.

Figura: Escala de avaliação de ameaças

[130] Ver Apêndice 3 (5) do CSD (Decreto de Segurança Cibernética)

Nível	Descrição
Baixo	**Vulnerabilidade não existe ou é pouco provável** que seja explorada. Estão em vigor medidas de segurança capazes de detectar possíveis vulnerabilidades ou possíveis tentativas de as explorar atempadamente.
Médio	**É pouco provável que a exploração da vulnerabilidade seja provável.** Estão em vigor medidas de segurança, cuja eficácia é regularmente verificada. A capacidade das medidas de segurança para detectar possíveis vulnerabilidades no tempo ou possíveis tentativas de ultrapassar as medidas é limitada. Não se conhecem tentativas bem sucedidas de ultrapassar as medidas de segurança.
Alto	**É provável que a exploração da vulnerabilidade seja muito provável**. Estão em vigor medidas de segurança, mas a sua eficácia não cobre todos os aspectos necessários e não é verificada regularmente. Tem havido algumas tentativas parcialmente bem sucedidas para ultrapassar as medidas de segurança.
Crítico	**A exploração da vulnerabilidade é muito provável ou mais ou menos certa. As** medidas de segurança não são implementadas ou a sua eficácia é severamente limitada. A eficácia das medidas de segurança não é verificada. As tentativas bem sucedidas de ultrapassar as medidas de segurança são conhecidas.

Figura: Escala de avaliação de vulnerabilidades

Nível	Descrição
Baixo	**O risco é** considerado **aceitável**.
Médio	**O risco pode ser reduzido por medidas menos exigentes** ou, em caso de maior intensidade de medidas, o risco é aceitável.
Alto	**O risco é inaceitável a longo prazo,** e devem ser tomadas medidas sistemáticas para o eliminar.
Crítico	**O risco é inaceitável,** e devem ser tomadas medidas para o eliminar imediatamente.

Figura: Escala para avaliação de risco

5.3 Política de segurança

Uma política de segurança é **um conjunto de políticas e regras que determinam a forma de assegurar a protecção dos bens.**

Por defeito, uma política de segurança assenta no facto de as entidades designadas serem obrigadas, no que diz respeito ao sistema de gestão da segurança da informação, a fazê-lo:

a) **estabelecer uma política de segurança** e **manter documentação de segurança** abrangendo as seguintes áreas políticas:[131]
    - sistema de gestão da segurança da informação,
    - gestão de activos,
    - segurança organizacional,

[131] Para mais detalhes, ver Apêndice 5 ao CSD

- gestão de fornecedores,
- segurança dos recursos humanos,
- gestão do tráfego e das comunicações,
- controlo de acesso,
- comportamento seguro dos utilizadores,
- backup e recuperação e armazenamento a longo prazo,
- transmissão segura e troca de informações,
- gestão de vulnerabilidades técnicas,
- utilização segura de dispositivos móveis,
- aquisições, desenvolvimento e manutenção,
- protecção de dados pessoais,
- segurança física,
- segurança da rede de comunicação,
- protecção contra código malicioso,
- implantação e utilização de uma ferramenta para a detecção de eventos de cibersegurança,
- utilização segura de protecção criptográfica,
- gestão da mudança,
- gestão de incidentes de ciber-segurança,
- gestão da continuidade de negócios.

O **conteúdo da documentação de segurança** também é especificado. Deve incluir:

- relatório de auditoria de ciber-segurança,
- relatório sobre a revisão do sistema de gestão da segurança da informação,
- metodologia para a identificação e avaliação de activos e para a avaliação de riscos,
- relatório de avaliação de activos e riscos,
- declaração de aplicabilidade,
- plano de gestão de risco,
- plano de desenvolvimento da sensibilização para a segurança,
- registos de alterações,
- dados de contacto comunicados,
- uma visão geral dos regulamentos jurídicos geralmente vinculativos, regulamentos internos e outros regulamentos e obrigações contratuais,
- outra documentação recomendada (por exemplo, topologia de infra-estruturas, visão geral dos dispositivos de rede).

b) **rever regularmente a política de segurança** e a **documentação de segurança,**

c) assegurar que a política de segurança e a documentação de segurança estejam actualizadas.

A política de segurança e a documentação de segurança devem ser:

- disponível em formato impresso ou electrónico,
- comunicado como parte de um devedor,
- razoavelmente disponíveis para as partes interessadas,
- gerido,
- protegidos em termos de confidencialidade, integridade e disponibilidade,
- mantidos de tal forma que a informação aí contida seja completa, legível, facilmente identificável e facilmente pesquisável.

5.4 Segurança organizativa

A definição da segurança organizacional e especialmente a ancoragem da segurança cibernética ou das TIC dentro das estruturas já em funcionamento de uma organização é da maior importância para a possível gestão de ameaças ou ataques cibernéticos.

As questões de segurança devem ser abordadas numa organização a nível operacional, táctico e estratégico, do ponto de vista da gestão da organização.

Do ponto de vista da segurança, é importante que o departamento de ciber-segurança seja separado do departamento que fornece as operações de TIC.[132]

Exemplo: O autor encontrou-se com um administrador de rede que foi obrigado pelo seu empregador a tornar-se ao mesmo tempo gestor de segurança. Na prática, isto significaria que o administrador elaboraria directivas a serem seguidas, ao mesmo tempo que verificava por si próprio o seu cumprimento e a sua aplicação. O absurdo desta situação é óbvio à primeira vista.

Por defeito, a segurança organizacional assenta no facto de que as entidades designadas são obrigadas, no que respeita ao sistema de gestão da segurança da informação, a fazê-lo:

- **assegurar que a política e os objectivos de segurança do SGSI** sejam estabelecidos de modo a serem compatíveis com a direcção estratégica do devedor,
- **assegurar a integração do SGSI** nos processos do devedor,
- **assegurar a disponibilidade** dos recursos necessários **para o SGSI**,
- **informar os trabalhadores da importância do SGSI** e da importância de conseguir o cumprimento dos seus requisitos com todas as partes interessadas,
- **fornecer apoio** para alcançar os resultados pretendidos do **ISMS,**
- **levar os empregados a desenvolver a eficiência do SGSI** e apoiá-los neste desenvolvimento,
- **promover a melhoria contínua do SGSI**,
- **apoiar os detentores de papéis de segurança** na promoção da ciber-segurança nas suas áreas de responsabilidade,
- **assegurar o estabelecimento de regras para a designação de administradores e pessoas que irão desempenhar funções de segurança**,

  As funções de segurança incluem:

[132] Cf. *Bezpečnostní role a jejich začlenění v organizaci.* [em linha]. [cit. 21/08/2018]. Disponível em: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf p. 3

- **Gestor de** Ciber-segurança,
- **Arquitecto de** Ciber-segurança,
- **Fiador de bens**,
- **Auditor de** Ciber-segurança.

▪ **assegurar que a confidencialidade** dos administradores e agentes de segurança seja mantida,

▪ **proporcionar às pessoas com funções de segurança os poderes** e recursos **adequados**, incluindo dotações orçamentais para desempenharem as suas funções e executarem tarefas relacionadas,

▪ **assegurar o teste de planos de continuidade de negócios, recuperação e processos de gestão de incidentes de ciber-segurança**.

Para atribuir e exibir (dentro de uma tabela) as responsabilidades de pessoas individuais (funções de segurança de acordo com o CSD) dentro de uma organização, recomenda-se a utilização da **matriz de responsabilidade RACI** (**matriz RACI).** RACI é um acrónimo de:

R - Responsável	quem é responsável pela execução da tarefa atribuída (dada actividade)
A - Responsável (ou aprovador)	que é responsável por toda a tarefa, ou pelo facto de o processo dado ser realizado como pré-definido
C - Consultado	que pode fornecer conselhos ou consultas valiosos para a tarefa mas não assume a responsabilidade pela execução do processo
I - Informado	quem deve ser informado sobre o progresso da tarefa ou decisões na tarefa

A regra é que apenas uma pessoa tem responsabilidade global (A - Responsabilidade) por uma determinada tarefa, as pessoas envolvidas (R - Responsabilidade) devem ser proporcionais à tarefa em questão. O método RACI é uma forma simples de um modelo de competência.[133]

Processos:	**Papéis:**	**Comité CS**	**Gestor de CS**	**Arquitecto CS**	**Auditor CS**	**Fiador de bens**
Gestão global e desenvolvimento da SC		**A**	**R**	**R**		**C**
Sistema de gestão da segurança da informação		**A**	**R**	**C**		**C**
Proposta de medidas de segurança		**C**	**A**	**R**		**C**
Implementação de medidas de segurança		**C**	**A**	**R**		**C**
Garantia de desenvolvimento, utilização e bens de segurança			**A**	**C**		**R**
Auditoria CS		**I**	**C**	**C**	**A/R**	**C**

Figura: Matriz RACI[134]

[133] Para mais detalhes ver, por exemplo, *Matice odpovědnosti RACI (RACI Responsibility Matrix).* [online]. [cit. 21/08/2018]. Disponível em: https://managementmania.com/cs/matice-odpovednosti-raci ou *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21/08/2018]. Disponível a partir de: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf p. 6

[134] A matriz RACI na descrição dos processos básicos associados às funções de segurança. As relações dos papéis e processos individuais de segurança podem variar dependendo da organização. *Bezpečnostní role a jejich začlenění v organizaci.* [em linha]. [cit. 21/08/2018]. Disponível em: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf p. 7

5.5. Gestão de activos

Um bem é qualquer coisa que tenha um certo valor para uma pessoa, organização ou estado.

Um bem pode ser uma coisa **tangível** (edifício, sistema informático, redes, energia, bens, etc.) ou **intangível** (informação, conhecimento, dados, programas, etc.) do ponto de vista do direito civil.

Contudo, um bem pode também ser uma **qualidade** (por exemplo, disponibilidade e funcionalidade do sistema e dos dados, etc.) ou um **bom nome**, reputação, etc. **As pessoas** (utilizadores, administradores, etc.), juntamente com os seus conhecimentos e experiência, são também uma mais-valia do ponto de vista da ciber-segurança.

Um **activo auxiliar** é um activo técnico, empregados e fornecedores envolvidos na operação, desenvolvimento, administração ou segurança do sistema de informação e comunicação.

Um **bem primário** é a informação ou um serviço processado ou fornecido por um sistema de informação e comunicação.

"Como parte de uma boa gestão da segurança da informação, é importante ter uma visão geral das ligações e dependências entre os bens primários e acessórios".[135]

Como parte da gestão de activos, as entidades são obrigadas a fazê-lo:

- **estabelecer uma metodologia para a identificação de bens**,
- estabelecer uma metodologia para a **valorização dos activos**,
- **identificar e registar bens**,
- **determinar** e registar **os fiadores de bens**,
- **avaliar e registar os bens primários** em termos de confidencialidade, integridade e disponibilidade e classificá-los em níveis individuais de bens,
- **determinar e registar as ligações entre bens primários e acessórios** e avaliar as consequências das dependências entre bens primários e acessórios,
- **avaliar os activos auxiliares** e ter em conta as interdependências entre os activos primários e auxiliares,
- estabelecer e **implementar as regras de protecção** necessárias para garantir os **vários níveis de bens**,
- estabelecer utilizações admissíveis para os bens e regras para o tratamento dos bens no que respeita ao nível dos bens, incluindo regras para a partilha electrónica segura e a transferência física de bens,
- determinar o método de eliminação de dados, dados operacionais, informações e respectivas cópias ou eliminação de suportes de dados técnicos no que diz respeito ao nível de bens.

Ao avaliar o significado dos bens primários, é obrigatório considerar:

- âmbito e importância dos dados pessoais, categorias especiais de dados pessoais ou segredos comerciais,
- âmbito das obrigações legais ou outras obrigações em questão,
- âmbito da violação das actividades internas de gestão e inspecção,

[135] MAISNER, Martin e Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praga: Wolters Kluwer, 2015. p. 85

- danos a interesses públicos, comerciais ou económicos e possíveis perdas financeiras,
- impacto na prestação de serviços importantes,
- âmbito da perturbação das actividades normais,
- impacto na manutenção da boa vontade ou na protecção da reputação,
- tem impacto na segurança e saúde das pessoas,
- impactos nas relações internacionais,
- impactos nos utilizadores do sistema de informação e comunicação.

5.6 Segurança dos recursos humanos

As entidades são também obrigadas a prestar atenção à segurança dos recursos humanos no âmbito do SGSI como um dos bens. Como mencionado anteriormente, as pessoas são normalmente o elo mais fraco da ciber-segurança. Em particular, estas entidades são obrigadas a fazê-lo:

- **estabelecer um plano de desenvolvimento da sensibilização para a segurança** para assegurar uma educação e melhoria adequadas da sensibilização para a segurança,

  Este plano contém a forma, conteúdo e âmbito de

  - instrução dos utilizadores, administradores, agentes de segurança e fornecedores sobre as suas responsabilidades e política de segurança;
  - formação teórica e prática necessária para utilizadores, administradores e agentes de segurança.
- **designar as pessoas responsáveis** pela execução das actividades individuais previstas no plano,
- **fornecer orientações** aos utilizadores, administradores, agentes de segurança e fornecedores sobre as suas responsabilidades e política de segurança através de formações iniciais e regulares,
- **proporcionar formação profissional regular a pessoas com funções de segurança**,
- assegurar **sessões regulares de formação** e verificação da consciência de segurança dos empregados, de acordo com a descrição das suas funções,
- assegurar a **verificação do cumprimento da política de segurança pelos utilizadores**, administradores e pessoas com funções de segurança,
- em caso de cessação da relação contratual com administradores e pessoas com funções de segurança, **assegurar a transferência de responsabilidades**,
- **avaliar a eficácia do plano de desenvolvimento da sensibilização para a segurança**, a formação ministrada e outras actividades relacionadas com a melhoria da sensibilização para a segurança,
- **determinar regras e procedimentos para lidar com violações das regras de segurança estabelecidas** por utilizadores, administradores e pessoas com funções de segurança.

É obrigatório manter uma visão geral das sessões de formação acima mencionadas que contenham o tema da formação e uma lista de pessoas que tenham completado a formação.

Exemplo: Uma vez que a formação padrão, que é a única que os utilizadores têm de completar, se revela ineficaz, algumas organizações também abordam métodos para verificar uma verdadeira compreensão da informação fornecida na sua própria formação. Isto poderia ser, por exemplo, o envio de mensagens de phishing aos utilizadores após uma formação centrada nesta área. A organização monitoriza então quantos utilizadores responderam incorrectamente ao ataque. No entanto, é de notar que tais testes devem ser bem pensados, e um advogado para avaliar se o teste utilizado não infringirá, por exemplo, a privacidade dos empregados não deve estar ausente.

5.7 Gestão da continuidade das actividades

Business Continuity Management (**BCM**) é um processo baseado na identificação de elementos-chave (sistemas e processos) numa organização e, em seguida, a criação de processos e procedimentos para assegurar a continuidade ou renovação desses elementos, a um nível pré-definido em que ainda será possível executar tarefas básicas da organização.

No caso da gestão da continuidade das actividades, deverá ser efectuada uma avaliação e análise dos riscos dos sistemas e serviços de informação e comunicação existentes e, com base nos dados assim obtidos, determinados:

- **o nível mínimo de serviços prestados**, que é aceitável para a utilização, funcionamento e gestão do sistema de informação e comunicação,
- **o tempo de restauração da operação**, durante o qual o nível mínimo de serviços do sistema de informação e comunicação fornecidos será restaurado após um incidente de ciber-segurança,
- **esse ponto de recuperação de dados** como o período de tempo durante o qual os dados devem ser recuperados após um incidente ou falha de ciber-segurança.

O devedor deve também no âmbito da gestão da continuidade das actividades:

- **estabelecer os direitos e obrigações** dos administradores e das **pessoas** com funções de segurança,
- avaliar e **documentar possíveis impactos de incidentes de cibersegurança e avaliar possíveis riscos** relacionados com ameaças à continuidade do negócio através da avaliação de riscos e análise de impacto,
- **estabelecer uma política de gestão da continuidade das actividades**,
- **desenvolver, actualizar e testar regularmente planos de continuidade de negócios e planos de emergência** relacionados com o funcionamento do sistema de informação e comunicação e serviços relacionados,
- **implementar medidas para aumentar a resistência do sistema de informação e comunicação** a incidentes de ciber-segurança e restrições à disponibilidade.

5.8 Medidas técnicas

As medidas técnicas juntamente com as medidas organizacionais são os elementos básicos das medidas de segurança. Enquanto as medidas organizacionais se concentram principalmente no estabelecimento de regras e políticas numa organização, as medidas técnicas concentram-se principalmente em regras para a criação de sistemas e serviços de informação e comunicação.

No âmbito de medidas técnicas individuais, serão também demonstradas possíveis ferramentas de fonte aberta aplicáveis à medida em questão.

5.8.1 Segurança física

A segurança física centra-se principalmente na protecção dos bens técnicos de uma determinada entidade. Relativamente à segurança física, Maisner afirma que "*o objectivo desta medida é principalmente impedir o acesso não autorizado a elementos individuais da infra-estrutura, salas de servidores, locais de trabalho dos administradores de sistemas, etc. O esforço é prevenir o roubo de bens directa e indirectamente relacionados com o sistema de informação, ou prevenir danos a equipamentos corpóreos e incorpóreos ou equipamento de espaços. Por último, mas não menos importante, tenta evitar uma fuga de informação e de dados.* "[136]

No âmbito da segurança física, o devedor deve

- **prevenir danos**, roubo ou má utilização de bens ou interrupção do fornecimento de serviços do sistema de informação e comunicação,
- determinar um **perímetro de segurança física** demarcando a área em que a informação é armazenada e processada e onde se encontram os bens técnicos do sistema de informação e comunicação,
- **aplicar meios de segurança física** ao perímetro físico:
    - **para impedir a entrada de pessoas não autorizadas,**
    - **para prevenir danos e interferências não autorizadas**,
    - **para proporcionar protecção ao nível do edifício e dentro dos edifícios.**

O termo **perímetro de segurança** física delineia um espaço designado ou os limites deste espaço. Tal espaço pode ser, por exemplo, um conjunto de instalações, as próprias instalações ou parte de uma instalação.

O local é um edifício ou outro espaço confinado. O **limite das instalações** significa um envelope de edifício, uma barreira física (vedação) ou outro limite visivelmente definido da área. Uma **área protegida** significa um espaço num edifício que está estruturalmente ou visivelmente delimitado de outra forma.

Os meios de segurança física podem incluir:

- **meios mecânicos de retenção** (por exemplo, fechaduras, portas, grades, folhas, vidros e outros elementos estruturais e de construção de segurança, cofres-fortes de armários, portas de segurança e cofres-câmara,
- **sistema de inspecção de acesso à área segura** [sistemas de alarme e de segurança electrónica, detectores (movimento, quebra de vidro, etc.) determinação das condições de entrada: elemento de identificação, PIN, biometria (ou uma combinação dos mesmos)],
- **equipamento de sinalização de segurança eléctrica** (sistemas de segurança de alarme e de emergência - painéis de controlo de sinalização de segurança eléctrica, detectores de sinalização de segurança eléctrica, detectores de choque, sistemas de detecção de perímetro, sistemas de emergência, etc.),
- **sistemas especiais de televisão** (**sistemas de câmaras**, sistemas de vigilância CCTV, etc.),
- **sistemas de detecção e alarme de incêndio** (ligação ao equipamento de controlo e alarme, ou ao painel de controlo do alarme de segurança eléctrica),

[136] MAISNER, Martin e Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praga: Wolters Kluwer, 2015. p. 91

- **equipamento que limita os efeitos dos incêndios e eventos naturais** (sistemas de alarme, detectores de fumo, sistemas de extinção automática de incêndios, etc.),
- **equipamento para assegurar protecção contra falha de alimentação** (fontes de alimentação de reserva - UPS, geradores diesel, etc.).

Também é possível implementar, por exemplo:

- **equipamento contra espionagem passiva e activa.**[137]

As áreas onde a entrada/acesso deve ser limitada ou regulada do ponto de vista da segurança dos sistemas de informação e comunicação, incluem principalmente **salas de servidores** (primária, backup), **espaços com elementos de rede** (router, switch, etc.), **armazéns de dados** (salas de arquivo, armazéns NAS, etc.), **instalações de administradores de TIC**, etc.

Exemplo: A segurança física é uma das áreas onde as regras organizacionais são tipicamente violadas e onde são necessárias auditorias periódicas. Enquanto a maioria das outras actividades na organização são realizadas por administradores, a gestão do acesso físico é confiada a uma força de trabalho menos qualificada após a implantação da segurança, por exemplo, por razões de custo-benefício. Esta força de trabalho pode não estar a par de questões particulares de segurança.

O autor passou por várias situações em que, após um certo período de tempo, uma pessoa responsável pela gestão do acesso físico começou a conceder acesso a pessoas que não deveriam ter tido acesso às áreas (por exemplo, salas de servidores), por exemplo, apenas porque um gestor sénior solicitou o acesso à área protegida, embora não tivesse privilégios suficientes para ser aprovado.

Como parte da segurança física, é também possível utilizar ferramentas de código aberto. Em particular, estes envolverão casos de *"implementação de balcões centrais de segurança, incluindo sistemas de vigilância por câmaras. Para este fim, podem ser utilizadas ferramentas concebidas para monitorizar elementos da rede (**Icinga, Nagios** e outros), complementadas por uma interface para sensores correspondentes, ligados a programas de transmissão e captura de sinais de vídeo de câmaras de segurança".*[138]

5.8.2 Ferramenta para proteger a integridade das redes de comunicação

No âmbito da segurança física, alguns administradores são obrigados a fazê-lo:

- **assegurar a segmentação da rede de** comunicação,
- assegurar a gestão da comunicação dentro da rede de comunicação e do perímetro da rede de comunicação (ou seja, **gerir o acesso seguro entre a rede interna e externa**),
- **utilizar criptografia para assegurar a confidencialidade e integridade dos dados durante o acesso remoto**, a **administração** remota **ou o acesso** à **rede de** comunicações **utilizando**

---

[137] A área deve ser protegida contra escutas passivas e activas por paredes, portas, chão e tecto suficientemente insonorizados, janelas, aberturas de ventilação ou condutas de ar condicionado devem ser protegidos por meios técnicos. A área deve ser protegida contra espionagem a partir do exterior da área de reuniões. Nenhum mobiliário ou equipamento pode ser colocado na área, a menos que tenham sido inspeccionados para a utilização não autorizada de meios técnicos de obtenção de informações na área de reunião. O mobiliário e equipamento da área deve ser registado (incluindo o tipo, ou número de série e inventário), incluindo o histórico de movimento. Não é desejável a colocação de telefones na área. Se a sua instalação for absolutamente necessária, devem ser equipados com um desligador ou desconectados manualmente antes da reunião. Os telemóveis, qualquer aparelho de gravação, equipamento de transmissão, qualquer equipamento de teste, medição e diagnóstico e outro equipamento electrónico não podem ser trazidos para a área. (Isto não se aplica ao equipamento utilizado no decurso da inspecção com o conhecimento da pessoa responsável ou da sua pessoa autorizada). Devem ser elaboradas regras para o registo e circulação de pessoas e instalações para a área.

[138] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https:**//www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf**

tecnologias sem fios (ou seja, utilizar criptografia para assegurar, por exemplo, VPN, ligação ICT a Wi-Fi, etc.),

- **bloquear activamente a comunicação indesejada** (por exemplo, filtros de spam, etc.),
- para assegurar a segmentação da rede e gerir a comunicação entre os seus segmentos, utilizar um instrumento que assegure a protecção da integridade da rede de comunicação.

*"A ferramenta para proteger a integridade das redes de comunicação significa aqui uma **topologia de rede adequadamente concebida**, incluindo a utilização de elementos de rede que permitam a segmentação de rede necessária e a filtragem do tráfego entre elementos individuais. O equipamento utilizado para alcançar estes requisitos são comutadores Ethernet, routers e firewalls. Se não for possível assegurar a segmentação da rede utilizando uma VLAN num switch editável, é possível assegurar a sua segurança utilizando vários switches mais pequenos não gerenciáveis, cada um dos quais implementa uma LAN física.*

Ao segmentar algumas redes, é possível utilizar, por exemplo, os routers Turris (https://www.turris.cz/cs/), onde é garantida uma alta segurança (entre outras coisas devido ao firmware, que foi concebido no que diz respeito e para alcançar a máxima segurança possível) e também um baixo consumo de energia.

***Roteadores/firewalls de** software: www.ipcop.org/; https://www.ipfire.org/*

***Comutador** Ethernet para ambiente virtualizado: http://www.openvswitch.org/".*[139]

5.8.3 Ferramenta para verificação da identidade do utilizador

Como parte da segurança física, alguns administradores são obrigados a utilizar uma ferramenta para gerir e verificar a identidade dos utilizadores, administradores e aplicações de sistemas de informação e comunicação.

Esta ferramenta é actualmente um componente de todos os sistemas operativos comummente utilizados (Linux, iOS, Windows). Segundo o CSD, esta ferramenta deve assegurar

- **verificação da identidade pessoal** (antes de iniciar as actividades no sistema de informação e comunicação),
- **gestão do número** de possíveis **tentativas de login** falhadas,
- **resiliência** dos **dados de autenticação** armazenados ou transmitidos **contra roubo e utilização indevida não autorizada**,
- **armazenamento de** dados de **autenticação de** uma forma resistente a ataques offline,
- **re-verificação da identidade** após um período especificado de inactividade,
- **a observância da confidencialidade dos dados de autenticação** ao restaurar o acesso,
- **gestão centralizada da identidade.**

Para verificar a identidade dos utilizadores, administradores e aplicações, o devedor utiliza:

1. um **mecanismo de autenticação** que não se **baseia** apenas na utilização de um identificador e senha de conta, mas **na autenticação multi-factor, com pelo menos dois tipos diferentes de factores,**

[139] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

2. uma ferramenta para verificar a identidade dos utilizadores, administradores e aplicações, para utilizar **autenticação criptográfica de chaves** e garantir um nível de segurança semelhante[140],
3. uma ferramenta de verificação de identidade de utilizadores, administradores e aplicações que utiliza um **identificador de conta e uma palavra-passe para autenticação**.[141]

Se uma conta e senha forem utilizadas para autenticação, as seguintes condições devem ser satisfeitas:

- comprimento mínimo da palavra-passe:
  - **12 caracteres para utilizadores** e
  - **17 caracteres para administradores e aplicações**.
- **possibilidade de introduzir uma palavra-passe de pelo menos 64 caracteres,**
- possibilidade de utilizar **letras minúsculas e maiúsculas, números e caracteres especiais** numa palavra-passe,
- **possibilidade de alterar uma senha**, enquanto que **o tempo entre duas alterações de senha não deve ser inferior a 30 minutos**,
- **não permitir que utilizadores e administradores o façam:**
  - **escolher as palavras-passe mais frequentemente utilizadas,**
  - **criar senhas baseadas em** múltiplos caracteres repetitivos, nome de login, e-mail, nome do sistema ou semelhante,
  - reutilizar palavras-passe usadas anteriormente com uma **memória de pelo menos 12 palavras-passe anteriores**.
- **alteração obrigatória de uma palavra-passe a intervalos máximos de 18 meses**, enquanto que esta regra não se aplica às contas utilizadas para recuperar o sistema em caso de catástrofe,
- **forçar a alteração da palavra-passe por defeito imediatamente após a sua primeira utilização,**
- **revogar imediatamente uma senha utilizada para restabelecer o acesso após a sua primeira utilização ou após um máximo de 60 minutos da sua criação,**
- **incluir regras para a criação de palavras-passe seguras no plano de desenvolvimento da sensibilização para a segurança**.

Exemplo: Recomendamos a utilização de demonstrações práticas para a formação de utilizadores. Por exemplo, as ferramentas CEWL ou CUPP. Ambas podem ser encontradas, por exemplo, na distribuição Linux Kali. A ferramenta CEWL pode criar um dicionário para um ataque de dicionário adaptado a uma organização específica, com base no conteúdo do seu website. A ferramenta CUPP pode então criar um dicionário à medida de um utilizador específico. De acordo com a experiência dos autores, estes exemplos práticos são muito benéficos para os utilizadores, uma vez que estes vêem praticamente que a sua palavra-passe utilizada até agora, que consiste, por exemplo, na data de nascimento e no nome do cão da família, pode efectivamente ser gerada se o atacante tiver informação suficiente sobre eles.

"Para autenticação prática do utilizador, a comunidade de código aberto oferece muito software compatível com os seus equivalentes comerciais. Estes são, por exemplo:

[140] Desde que o devedor ainda não tenha cumprido o primeiro dos mecanismos de autenticação preferidos.
[141] Desde que o devedor ainda não tenha cumprido o segundo dos mecanismos de autenticação preferidos

FreeRADIUS - http://freeradius.org/ /RADIUS

OpenLDAP - http://www.openldap.org/ /Microsoft AD, Oracle Internet Directory

Kerberos - https://www.gnu.org/software/shishi/

OpenDiameter - https://sourceforge.net/projects/diameter/

Todas estas ferramentas fornecem meios para impor a complexidade da palavra-passe especificada, bem como outros atributos exigidos pela CSA, quer por eles próprios através do login.conf*, quer utilizando mecanismos externos tais como cracklib e dicionários de "palavras-passe" populares.*[142]

5.8.4 Ferramenta de gestão de permissões de acesso

No âmbito da segurança física, alguns administradores são obrigados a utilizar uma ferramenta centralizada de gestão de permissões de acesso.

O termo **permissão** significa o direito de acesso a qualquer dos bens (tipicamente um sistema de informação ou comunicação, aplicações, etc.). Na prática, é uma ferramenta para "gestão de utilizadores e grupos" e uma ferramenta para definir permissões em ficheiros e directórios. Estas ferramentas são um componente proprietário de todos os sistemas operativos padrão.

Um instrumento centralizado de gestão de permissões de acesso destina-se a assegurar a gestão das permissões:

- para o acesso aos bens individuais do sistema de informação e comunicação e
- para ler dados, escrever dados e alterar permissões.

É aconselhável aplicar ferramentas de gestão centralizada dos direitos de acesso **que comunicarão com um servidor central AAA** (Autenticação, Autorização, Contabilidade).

Exemplo: É importante ter em mente a gestão das permissões de acesso ao conceber software. O autor conhece uma aplicação que tinha permissões muito gerais, e de facto apenas existiam nela os papéis de administrador e utilizador. O administrador foi autorizado a acrescentar utilizadores e administradores adicionais, e o utilizador foi autorizado a realizar outras actividades. No entanto, esta aplicação armazenou informações importantes sobre os clientes da organização. Uma vez que esta aplicação não permitia qualquer granularidade de permissões, todos os utilizadores, independentemente das suas necessidades empresariais reais, eram autorizados a aceder a qualquer parte da informação sobre os clientes. Esta situação acabou por resultar numa fuga de dados relacionados com um cliente específico.

5.8.5 Ferramenta de protecção contra malware

Como parte da segurança física, alguns administradores são obrigados a estabelecer uma protecção contra códigos maliciosos:

- **assegurar** (dada a importância dos bens) **a utilização de um instrumento de protecção automática contínua de**
  - estações terminais,
  - dispositivos móveis,
  - servidores,

---

[142] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

   - armazenamentos de dados e suportes de dados amovíveis,
   - redes de comunicação e elementos da rede de comunicação,
   - dispositivos semelhantes.
- **monitorização e gestão da utilização de dispositivos amovíveis e suportes de dados,**
- **monitorização e gestão da utilização de** dispositivos amovíveis e suportes de dados,
- **gerir as permissões de execução do código,**
- **realizar uma actualização regular e eficaz** de uma ferramenta anti-malware.

*"**Protecção contra software malicioso distribuído através de correio electrónico.** Uma solução proxy de e-mail de código aberto que fornece protecção contra software malicioso é o projecto ASSP (AntiSpam SMTP Proxy, https://sourceforge.net/projects/assp/), que permite uma configuração abrangente do comportamento de proxy de e-mail através de uma interface web.*

__Protecção contra software malicioso distribuído via web.__ Uma solução adequada é, por exemplo, o projecto HTTP AntiVirus Proxy (http://www.havp.org/) ou www.cacheguard.com. Também aqui é necessário assegurar uma protecção adequada das estações de trabalho finais, pois o tráfego encriptado não pode ser digitalizado em tempo real na posição "homem no meio".

Bloqueio do tráfego da sua rede, tanto ao nível da infra-estrutura de dados como ao nível de "firewalls pessoais" das estações finais. As regras de comunicação da rede devem ser definidas "de forma paranóica", ou seja, para permitir apenas o tráfego necessário para que o software legítimo funcione e proibir todo o resto. Contudo, a medida de um servidor, servidor proxy ou elemento de infra-estrutura de rede não substitui de forma alguma a protecção contra malware nas estações de trabalho endpoint, especialmente porque nem sempre pode interceptar tráfego encriptado que é desencriptado apenas no programa cliente".[143]

5.8.6 Ferramenta para a detecção de eventos de ciber-segurança

No âmbito da segurança física, alguns administradores são obrigados a implementar, dentro de uma rede de comunicação que inclui um sistema de informação e comunicação, uma ferramenta de detecção de eventos de ciber-segurança que assegure:

- **verificação e verificação dos dados transmitidos dentro da rede de comunicação** e entre redes de comunicação,
- **verificação e verificação dos dados transmitidos no perímetro** da rede de comunicação e
- **bloqueio de comunicações indesejadas**.

"As saídas de muitas ferramentas de software podem ser utilizadas para detectar eventos de cibersegurança, incluindo analisadores de registo, tais como Logwatch (https://sourceforge.net/projects/logwatch/files/), Epylog (https://fedoraproject.org/wiki/Infrastructure/Fedorahosted-retirement), sistemas de detecção de intrusão, tais como OpenVAS (http://openvas.org/), Suricata (https://suricata-ids.org/), Snort (https://www.snort.org/) ou Samhain (-lasamhna.de/Samoin)".[144]

[143] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf
[144] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

5.8.7 Ferramenta para recolher e avaliar eventos de ciber-segurança

No âmbito da segurança física, alguns administradores são obrigados a utilizar uma **ferramenta para recolher e avaliar continuamente eventos de ciber-segurança.** Esta permite

- **a recolha e avaliação dos eventos**,
- **pesquisa e agrupamento de registos relacionados,**
- **fornecimento de informações para funções de segurança designadas** sobre eventos de cibersegurança detectados,
- **avaliação de incidentes de cibersegurança, a fim** de identificar incidentes de cibersegurança, incluindo o alerta precoce de funções de segurança identificadas,
- redução dos casos de avaliação incorrecta de eventos através da actualização regular das definições de regras para:
    - avaliação de eventos de ciber-segurança,
    - aviso prévio,
- utilização de informações obtidas por um instrumento de recolha e avaliação de eventos de ciber-segurança para o estabelecimento óptimo de medidas de segurança do sistema de informação e comunicação.

A ferramenta de recolha e avaliação de eventos de cibersegurança significa ferramentas que são referidas como **SIEM** (Security Incident and Event Management - Gestão de Incidentes e Eventos de Segurança).

Dentro da solução de código aberto SIEM, é possível utilizar, por exemplo, OSSIM/USM (https://www.alienvault.com/products/usm-anywhere/try-it-now), OSSEC (www.ossec.net/) ou logalyze (www.logalyze.com).[145]

5.8.8 Segurança da aplicação

No caso da segurança das aplicações, é dada atenção às aplicações que são utilizadas em sistemas de informação (seja dentro de um sistema informático, dispositivo móvel ou como uma aplicação web). A segurança das aplicações é assegurada, entre outras coisas, por testes de penetração de aplicações ou firewalls de aplicações.

Como parte da segurança física, alguns administradores são obrigados a realizar **testes de penetração** do sistema de informação e comunicação, concentrando-se em activos importantes, nomeadamente:

- **antes de serem postos em serviço e**
- **em ligação com uma mudança significativa**.

No âmbito da segurança dos pedidos, o devedor deve também **assegurar a protecção permanente dos pedidos, informações e transacções contra:**

- actividade não autorizada,
- negação das actividades realizadas.

"Firewalls de aplicação incluem, por exemplo, módulos de segurança de servidores web (www.modsecurity.org) ou OWASP Web Application Firewall. As ferramentas comerciais para testar

[145] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

a segurança das aplicações incluem, em particular, a ferramenta Nessus -(www.tenable.com/products/nessusvulnerabilityscanner). A -sua alternativa de código aberto é o projecto Open-VAS (www.openvas.org/)".[146]

5.8.9 Meios criptográficos

A criptografia (encriptação) é uma disciplina científica que trata da conversão de informação inteligível numa forma incompreensível para um destinatário se o destinatário não possuir as chaves com as quais é possível decifrar a informação.

Com a transferência de uma quantidade considerável de dados e informações para sistemas de TIC, é necessário prestar maior atenção às possibilidades de encriptação (confidencialidade do conteúdo) dos dados transmitidos.

No âmbito da segurança física, alguns administradores são obrigados, para proteger os bens do sistema de informação e comunicação, a

- utilizar algoritmos criptográficos e chaves criptográficas actualmente robustos,
- utilizar um sistema de gestão de chaves e certificados que:
    - assegura a geração, distribuição, armazenamento, alterações, restrições de validade, revogação de certificados e eliminação de chaves,
    - permite a inspecção e auditoria.
- promover o manuseamento seguro de meios criptográficos,
- ter em conta as recomendações no domínio dos meios criptográficos emitidas pelo Gabinete (NÚKIB), publicadas no seu sítio web.

*"A fim de assegurar uma cifragem suficientemente robusta do tráfego de rede, são utilizadas as bibliotecas OpenSSL (*openssl.org*), mas é necessário assegurar que estejam actualizadas e devidamente configuradas de modo a cumprir com os termos deste decreto. É necessário seguir os relatórios actuais sobre vulnerabilidades e actualizar sem demora as versões insatisfatórias das bibliotecas para variantes sem vulnerabilidades conhecidas. A este respeito, recomenda-se o projecto Bettercrypto (https://bettercrypto.org/), para ajudar os administradores a garantir a melhor segurança possível para os serviços e a criptografia que utilizam".*[147]

5.8.10 Ferramenta para assegurar o nível de disponibilidade da informação

No âmbito da segurança física, alguns administradores são obrigados a implementar medidas para assegurar o nível de disponibilidade para garantir:

- **disponibilidade do sistema de informação e comunicação,**
- **resiliência do sistema de informação e comunicação** a incidentes de ciber-segurança que poderiam reduzir a sua disponibilidade,
- **disponibilidade de importantes recursos técnicos** do sistema de informação e comunicação,
- **redundância de bens** necessária para assegurar a disponibilidade do sistema de informação e comunicação.

---

[146] Ibidem

[147] KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* **[online]. [cit. 25/04/2018].** Disponível em: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

A implementação de uma ferramenta para assegurar o nível de disponibilidade de informação cumpre um trunfo organizacional: a Gestão da Continuidade da Empresa (**GCN**).

"Para atingir o nível de disponibilidade prescrito, podem ser utilizadas tecnologias de cluster e de nuvem desenvolvidas como fonte aberta (KVM, OpenStack), ou a disponibilidade de um activo de substituição pode ser assegurada num determinado momento através de software de back-up/restore (https://sourceforge.net/projects/bacula/)".[148]

[148] Ibidem

RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

- Há muitas razões para a introdução e implementação da ciber-segurança. As mais comuns incluem, por exemplo, consequências económicas negativas no caso de um ciberataque bem sucedido em que os dados sensíveis são roubados. Um ciberataque bem sucedido pode também comprometer as próprias operações e o funcionamento de uma organização, por exemplo, restringindo o acesso a sistemas informáticos ou a dados através de resgates. Outra razão para a introdução da ciber-segurança pode também ser a perda de credibilidade de uma organização atacada.
- Actualmente, o documento mais importante da União Europeia relacionado com a questão da ciber-segurança é a DIRECTIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO, de 6 de Julho de 2016, relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação em toda a União Europeia.
- O Sistema de Gestão da Segurança da Informação (SGSI) é um conjunto de regras concebidas para manter a confidencialidade, integridade e disponibilidade da informação, aplicando um processo de gestão de risco e dando garantias às partes interessadas de que os riscos estão a ser geridos adequadamente.
- A solução ISMS requer uma abordagem sistémica e abrangente, respeitando os princípios e elementos de todo o ciclo de vida da ciber-segurança. O sistema de gestão do SGSI baseia-se no ciclo de Deming, ou também no ciclo PDCA (Plan-Do-Check-Act).
- O ciclo PDCA é um dos princípios básicos de gestão baseado na melhoria gradual da qualidade dos processos, serviços, dados, produtos, etc., graças à repetição constante das suas quatro actividades básicas: Plan-Do-Check-Act.
- O valor do risco é mais frequentemente expresso como uma função afectada pelo impacto, ameaça e vulnerabilidade. Por exemplo, a seguinte função pode ser utilizada para a auto-avaliação do risco:
    - Risco = impacto * ameaça * vulnerabilidade
- Uma política de segurança é um conjunto de políticas e regras que determinam a forma de assegurar a protecção dos bens.
- A definição da segurança organizacional e especialmente a ancoragem da segurança cibernética ou das TIC dentro das estruturas já em funcionamento de uma organização é da maior importância para a possível gestão de ameaças ou ataques cibernéticos.
- Um bem é qualquer coisa que tenha um certo valor para uma pessoa, organização ou estado.
- Um activo auxiliar é um activo técnico, empregados e fornecedores envolvidos na operação, desenvolvimento, administração ou segurança do sistema de informação e comunicação.
- Um bem primário é a informação ou um serviço processado ou fornecido por um sistema de informação e comunicação.
- Business Continuity Management (BCM) é um processo baseado na identificação de elementos-chave (sistemas e processos) numa organização e, em seguida, a criação de processos e procedimentos para assegurar a continuidade ou renovação desses elementos, a um nível pré-definido em que ainda será possível executar tarefas básicas da organização.

PALAVRAS-CHAVE A LEMBRAR

- Directiva SRI
- ISMS
- PDCA
- Ameaça
- Risco
- Impacto
- Vulnerabilidade
- Política de segurança
- Bens
- Segurança física
- Gestão da Continuidade do Negócio

PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- Definir ISMS.
- O que é o ciclo PDCA, e como é que se aplica?
- Que componentes podem ser incluídos na segurança física?
- O que é: Gestão da Continuidade do Negócio?
- Definir ameaça.
- Definir o risco.
- Definir o impacto.
- Definir vulnerabilidade.
- Definir activo.
- Que bens reconhecemos, e que tudo é um bem?

6. Protecção de dados pessoais no ciberespaço

Em primeiro lugar, quero concentrar-me na protecção dos indivíduos, especificamente na protecção da forma e da privacidade do indivíduo. A privacidade é um dos direitos humanos fundamentais consagrados na Declaração Universal dos Direitos do Homem de 1948[149] .

6.1 Excursão nos direitos e obrigações decorrentes de certas normas legais

Estamos absolutamente convencidos de que **não é apropriado abordar separadamente a questão da ciber-segurança e outras áreas de segurança** (por exemplo, protecção de dados pessoais, dados relacionados com comunicações electrónicas e outros dados semelhantes).

A razão desta crença reside na crescente integração e interligação de diferentes categorias de dados com sistemas e aplicações informáticas que neles correm. Esta interligação e digitalização de dados analógicos só irá aumentar no futuro.

Por esta razão, parece ser um ponto de partida adequado para abordar a questão da segurança de forma abrangente e não apenas em relação aos direitos e obrigações decorrentes da Lei de Segurança Cibernética ou de outra legislação.

O objectivo das organizações ou indivíduos deve ser o de implementar tais regras, processos, procedimentos e medidas de segurança que satisfaçam os requisitos do SRI, bem como, por exemplo, GDRP, ePrivacy, eIDAS, etc. Tal procedimento permitirá a criação de uma **segurança integrada**.[150]

---

[149]Disponível a partir de: http://www.osn.cz/wp-content/uploads/2015/03/vseobecna-deklarace-lidskych-prav.pdf
Estes direitos estão principalmente consagrados nos artigos 12º e 18º da Declaração Universal dos Direitos do Homem.
Artigo 12: *"**Ninguém será sujeito a interferências arbitrárias na sua privacidade**, família, casa **ou correspondência**, nem a ataques à sua honra e reputação. **Todos têm direito à protecção da lei contra tais interferências ou ataques.*** ”
Artigo 18: *"Toda a pessoa tem direito à liberdade de pensamento, consciência e religião; este direito inclui a liberdade de mudar a sua religião ou crença, e a liberdade, quer sozinha ou em comunidade com outros e em público ou privado, de manifestar a sua religião ou crença no ensino, na prática, no culto e na observância".*

[150] Para mais detalhes, ver por exemplo GREENFIELD, David. *Integrovaná bezpečnost: Uz nastal její čas?* [online]. [cit. 01/03/2018]. Disponível a partir de: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

Figura: Demonstração de soluções de segurança integradas[151]

Segurança multidisciplinar integrada

Řízení rizik a soulad s právními předpisy	**Gestão de riscos e cumprimento da legislação**
Právní poradenství pro bezpečnost	Aconselhamento jurídico para a segurança
Finanční analýza bezpečnostních aspektů	Análise financeira dos aspectos de segurança
Reakce na bezpečnostní incidenty a řízení incidentů	Resposta e gestão de incidentes de segurança
Bezpečnostní audity, soulad s požadavky ZoKB, eIDAS, GDPR, ČNB, PCI DSS, ISO27k	Auditorias de segurança, conformidade com os requisitos CSA, eIDAS, GDPR, CNB, PCI DSS, ISO27k
Analýza rizik	Análise de risco
Obnova po havárii	Recuperação em caso de catástrofe
Řízení informační bezpečnosti	Gestão da segurança da informação
Řízení kontinuidade činnosti organizace	Gestão da continuidade do negócio
Řízení fyzické bezpečnosti	Gestão da segurança física
Zabezpečení provozu	**Segurança do tráfego**
Forenzní sluzby	Serviços forenses
Specializovaná bezpečnostní školení a předávání know-how	Formação especializada em segurança e transferência de know-how
Mobilní bezpečnost, MDM, BYOD	Segurança móvel, MDM, BYOD
Řízení přístupů a identit, Identity-as-a-Service	Acesso e gestão da identidade, Identidade como Serviço
Pokročilá analytika pro bezpečnost, predikce, predikce, učící se stroje	Análises avançadas para segurança, previsão, aprendizagem de máquinas
Zpravodajství a ochrana kybernetického prostoru	Inteligência e protecção do ciberespaço
Bezpečnost z technologického hlediska	**Segurança de um ponto de vista tecnológico**
Bezpečnost Cloudů Cloudů	Segurança nas nuvens
Bezpečnost datových center a sdílených sluzeb	Segurança dos centros de dados e serviços partilhados
Posouzení a audit ICS/SCADA systémů	Avaliação e auditoria dos sistemas ICS/SCADA
Zabezpečení průmyslových zařízení a IoT, Průmysl 4.0	Segurança das instalações industriais e da IOT, Indústria 4.0

[151] *Integrovaná multidisciplinární bezpečnost.* [online]. [cit. 17/02/2018]. Disponível a partir de: https://www2.deloitte.com/cz/cs/pages/risk/solutions/integrovana-multidisciplinarni-bezpecnost.html

Systémy distribuované důvěry a Blockchain	Sistemas de confiança distribuídos e Blockchain
Kryptografie pós-kvantová kryptografie	Criptografia pós-quantum
Zabezpečení platebních a transakčních systémů	Segurança dos sistemas de pagamento e transacção
Bezpečnostní technologie a integrace (Monitorização, SIEM, SOC, DLP, řízení zranitelnosti)	Tecnologias de segurança e integração (Monitorização, SIEM, SOC, DLP, gestão de vulnerabilidades)
Bezpečnost Veřejně Veřejně regulovaných sluzeb (PRS) a satelitních technologiíí	Segurança dos Serviços Públicos Regulamentados (PRS) e tecnologias de satélite
Etický hacking	**Hacking ético**
Bezpečnostní revigorar kódu	Revisão do código de segurança
Penetrační testování	Teste de penetração
Red Teaming	Red Teaming

6.2 GDPR

O Regulamento Geral de Protecção de Dados (UE) 2016/679 ou o GDPR[152] é um dos mais importantes documentos jurídicos internacionais directamente relacionado com a questão da ciber-segurança, embora não se destine principalmente ao domínio das TIC.

> ***"GDPR ≠ IT + software.***
>
> *O novo regulamento de protecção de dados tem 778 linhas. Apenas 26 destas dizem directamente respeito à segurança informática. Tem alguma ideia do que os outros contêm"?*
>
> Mons. Eva Škorničková[153]

É a GDPR e a implementação das obrigações decorrentes deste regulamento que podem ser demonstradas pelo facto de ser apropriado abordar de forma abrangente as questões de segurança e não isolar artificialmente as obrigações decorrentes de várias normas legais (neste caso a Lei de Segurança Cibernética e a GDPR).

O objectivo desta publicação não é realizar uma análise separada e abrangente das questões relativas ao GDPR. Apenas serão definidos aqui termos, direitos e obrigações parciais decorrentes da GDPR que ao mesmo tempo tenham uma sobreposição no domínio da ciber-segurança.

O Regulamento GDPR é um **quadro jurídico geral para a protecção de dados pessoais** válido e eficaz em toda a UE e, em certos casos, fora deste território. O principal objectivo da GDPR é assegurar uma protecção abrangente dos direitos das pessoas em causa contra o tratamento não autorizado dos seus dados e dados pessoais, encontrar um equilíbrio entre os interesses legítimos dos responsáveis pelo tratamento, dos processadores e das pessoas em causa, criar um sistema de aplicação uniforme da lei e um mecanismo de sanções único neste domínio, etc.

O âmbito da recolha e partilha de dados pessoais aumentou significativamente devido às tecnologias e serviços de informação e comunicação que lhes estão ligados. As tecnologias da informação e da comunicação permitem tanto às empresas privadas como às autoridades públicas utilizar dados pessoais numa medida sem precedentes no exercício das suas actividades. Por outro lado, é também possível observar a divulgação voluntária massiva de dados pessoais por pessoas singulares a cujos dados isto se aplica.

As tecnologias de informação e comunicação mudaram significativamente a economia e a vida social. Devem facilitar a livre circulação de dados pessoais dentro da União Europeia e a transferência de tais dados para países terceiros e organizações internacionais. Ao mesmo tempo, porém, estas tecnologias

[152] [em linha]. Disponível a partir de: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&qid=1488972453767&from=CS

[153] ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10/11/2017]. Disponível a partir de: https:*//www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

e os processos a elas associados devem assegurar um elevado nível de protecção de dados pessoais. [154]

Devido ao acima exposto, porém, **surge** um **paradoxo interessante**, que consiste nos seguintes pontos:

- **pessoas singulares por si próprias publicam voluntariamente uma quantidade cada vez maior de dados sobre si próprias** (fotos, vídeos, etc.), utilizando normalmente serviços da sociedade da informação baseados no EULA[155] ou SLA[156] entre um utilizador e um fornecedor de serviços para distribuir estes dados,
- **os dados pessoais são na sua maioria publicados nas redes sociais**, o que, pela natureza do seu funcionamento, pressupõe tal divulgação e consagra nos Termos de Serviço as regras com base nas quais tais dados são tratados,
- **ao utilizar uma série de serviços da sociedade da informação, as pessoas singulares assumem, e muitas vezes esperam, a interacção entre estas tecnologias e a sua personalidade cibernética**[157] .
- a comunidade internacional, o Estado e as próprias **pessoas singulares exigem maior segurança dos dados pessoais e a negação de acesso a estes dados a outras entidades** (geralmente não autorizadas)**, desde que se mantenha a existência dos três primeiros pontos deste paradoxo.**

A consequência deste paradoxo é óbvia. Os prestadores de serviços da sociedade da informação[158] devem, portanto, envidar maiores esforços para garantir os serviços individuais que prestam ao utilizador final, para aumentar o nível de segurança dos dados relacionados com o utilizador, para modificar os Termos de Serviço existentes e para introduzir requisitos adicionais decorrentes do GDPR.

6.2.1 Âmbito territorial do PIBR

Poder-se-ia pensar que uma forma de evitar o GDPR seria ir além do seu alcance, ou seja, fora do território da UE. No entanto, o GDPR aplica-se nos casos em que:

---

[154] Cf. considerando 6 do PIBR

[155] **EULA** (End Users Licence Agreement) significa os Termos de Serviço que permitem a utilização de um serviço de um prestador de serviços. O EULA é um contrato que é normalmente definido unilateralmente por um prestador de serviços. No entanto, um utilizador não está de forma alguma limitado nos seus direitos, uma vez que tem a opção de não utilizar tais termos de serviço definidos unilateralmente. No caso de consentimento para a utilização de tais serviços, é geralmente possível afirmar que as normas de direito privado serão aplicadas principalmente.
A questão é saber se um utilizador está realmente ciente dos Termos de Serviço com os quais concordou, quando estes se tornam vinculativos para ele e que possível interferência (legal) nos seus direitos humanos e liberdades fundamentais é tal consentimento. Outro facto importante é que o serviço prestado desta forma pode afectar os direitos e interesses legítimos (por exemplo, segurança informática, fiabilidade dos dados, etc.) de terceiros (por exemplo, empregadores, etc.) que não tenham concordado explicitamente em utilizar o serviço.
O triste facto é que uma percentagem muito pequena de utilizadores está disposta a ler os Termos de Serviço relativos a um serviço prestado.

[156] **SLA (**Service-Level Agreement) significa um acordo celebrado por e entre um prestador de um serviço e o seu utilizador.

[157] **Esta interacção pode ser monitorizada quando se utilizam serviços de localização e geolocalização** (por exemplo, Google Maps, Waze, Map List, etc.) uma vez que uma pessoa singular assume que o sistema informático será capaz de o localizar e mostrar o percurso mais conveniente. Do mesmo modo, a interacção é esperada, por exemplo, **para serviços que permitam a venda e compra de bens** (por exemplo, Letgo - ver anúncios recomendados por geolocalização ou bens já adquiridos), **serviços de restauração e alojamento** (por exemplo, Tripadvisor, Booking.com, Airbnb, etc.), etc.

[158] Para mais detalhes ver KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 78 e seguintes e p. 109 e seguintes.

- **um controlador ou processador está estabelecido na UE**, independentemente de o processamento ter lugar na UE,
- **os controladores ou processadores não estão estabelecidos na UE, mas**
    - os bens ou serviços são oferecidos às pessoas em causa na UE (independentemente da remuneração),
    - a conduta das pessoas em causa dentro da UE é monitorizada.[159]

Devido ao âmbito territorial assim definido, o GDPR tem um impacto extraterritorial e aplicar-se-á efectivamente a todos os serviços da sociedade da informação que podem ser acedidos a partir do território geográfico da UE ou que monitorizam a conduta das pessoas em causa no interior da UE.

6.2.2 Dados pessoais

Nos termos do artigo 4 (1) da GDPR, os dados pessoais são "***qualquer informação relativa a uma pessoa singular identificada ou identificável".*** *Uma pessoa singular identificável é aquela que pode ser identificada, directa ou indirectamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou a um ou mais factores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".*

De acordo com o GDRP, dados pessoais são **qualquer informação** (por exemplo, pictórica, escrita, verbal, digital, genética, médica, etc.) que **esteja relacionada** (por conteúdo - por exemplo, nome, morada, cargo, e-mail, etc.) **a um sujeito dos dados**.[160] Deste ponto de vista, e em conformidade com a interpretação dada nos considerandos 30, 34, 35 e 38 da GDPR[161] , os seguintes dados devem ser considerados como dados pessoais:

- nome e sobrenome,
- **número de identificação,**
- número da certidão de nascimento,
- **dados de localização (geo-)**,
- idade e data de nascimento,
- género,
- estatuto pessoal,
- a cidadania,
- **identificadores de rede,**
    - **Endereço IP**,
    - **identificadores de biscoitos**,
    - etiquetas de identificação por radiofrequência, etc..,

---

[159] Ver artigo 3 do GDPR - Âmbito territorial

[160] De acordo com o artigo 4 (1) do GDPR, **a pessoa em causa** é uma **pessoa singular** identificada ou identificável. **Um sujeito pode ser identificado:**

- **directamente,**
- **indirectamente (por exemplo, singling out, etc.).**

[161] Os considerandos são disposições que precedem o texto real do GDPR e são, em alguns casos, uma interpretação ou, em certa medida, uma exposição de motivos do texto real do regulamento.

- **fotografia**,
- **elementos** de identidade física, fisiológica, genética, mental, económica, **cultural ou social,**
- endereço pessoal ou de trabalho,
- número de telefone pessoal ou de trabalho,
- **e-mail pessoal ou de trabalho,**
- **dados de identificação de verificação**,
- números de identificação emitidos pelo Estado.

Os dados pessoais arrojados estão tipicamente relacionados com as tecnologias de informação e comunicação, bem como com as aplicações que utilizam essas tecnologias. A expansão da gama de dados que podem ser considerados dados pessoais afecta significativamente as questões de ciber-segurança e a garantia da protecção dos dados que são geridos na organização.

Se nos concentrarmos no **item de identificadores de rede e dados de identificação de autenticação, descobriremos que uma série de dados que permitem o funcionamento básico de um sistema informático numa rede podem e provavelmente serão considerados dados pessoais.**

Há uma questão frequentemente discutida na prática - um endereço IP é um dado pessoal?

Neste caso, para além do GDPR, é adequado ter em conta a jurisprudência do Tribunal de Justiça da UE, que decidiu, inter alia, no caso: **Patrick Breyer** contra **República Federal da Alemanha.** [162]

Patrick Breyer exigiu nos tribunais alemães que a Alemanha deixasse de manter os seus endereços IP, que obteve durante as suas "visitas" a vários sítios web publicamente acessíveis das autoridades federais alemãs. Do ponto de vista das actividades dos operadores dos sites em questão, este foi um registo clássico dos serviços oferecidos por este ISP[163] .

Os tribunais alemães suspenderam o processo e submeteram a questão ao Tribunal de Justiça da UE para uma decisão prejudicial porque não houve uma interpretação uniforme do direito da UE no presente caso.

Em particular, é necessário proceder a partir de um critério "*objectivo"* ou "*relativo*" para que um único pormenor seja um dado pessoal e assim identificar uma pessoa específica.

O critério "objectivo" significa que dados tais como **endereços IP podem ser considerados como dados pessoais** processados por FSI de serviços sem ligação (por exemplo, por um operador de website), **mesmo que apenas um terceiro seja capaz de identificar um utilizador específico** (normalmente ligação FSI).

O critério "relativo" significa que **os endereços IP podem ser considerados dados pessoais para uma ligação ISP**, uma vez que permitem identificar a identidade de um utilizador, **mas já não para serviços ISP que, na realidade, apenas dispõem de informação sobre endereços IP e não sabem o nome do visitante.**

O Tribunal de Justiça da UE declarou que **é indiscutível que um endereço IP dinâmico não constitui informação sobre uma "pessoa identificada"**, uma vez que o **endereço não revela directamente**

---

[162] Para mais pormenores, ver: [online]. Disponível a partir de: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

[163] Sobre o próprio conceito de ISP, os direitos e obrigações dos ISP individuais, ver em mais detalhe, por exemplo, KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 78 e seguintes e p. 109 e seguintes.

a identidade do indivíduo proprietário do computador a partir do qual o website foi visitado **nem a identidade de qualquer outra pessoa que possa ter utilizado o computador.**

Por outro lado, o Tribunal (Segunda Secção) também declarou (e posteriormente decidiu) que um **endereço dinâmico** de um protocolo Internet **detido por um fornecedor de serviços de comunicação social em linha em relação ao acesso de uma pessoa a um sítio web** que foi disponibilizado ao público por esse fornecedor **constitui um dado pessoal** para esse fornecedor na acepção da alínea a) do artigo 2º da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, **desde que o fornecedor tenha à sua disposição meios legais que lhe permitam ter a pessoa em causa identificada através de outras informações à disposição do fornecedor de serviços Internet dessa pessoa.**

De acordo com este acórdão, datado de 19 de Outubro de 2016, um endereço IP dinâmico pode, em determinadas circunstâncias, ser um dado pessoal.

Demonstramos o impacto do facto de que um **endereço IP, bem como outros identificadores de rede, podem ser dados pessoais** em dois exemplos.

A figura seguinte mostra a comunicação de um PC e de elementos individuais da rede (AP, servidor DHCP) e a subsequente ligação do PC à rede.

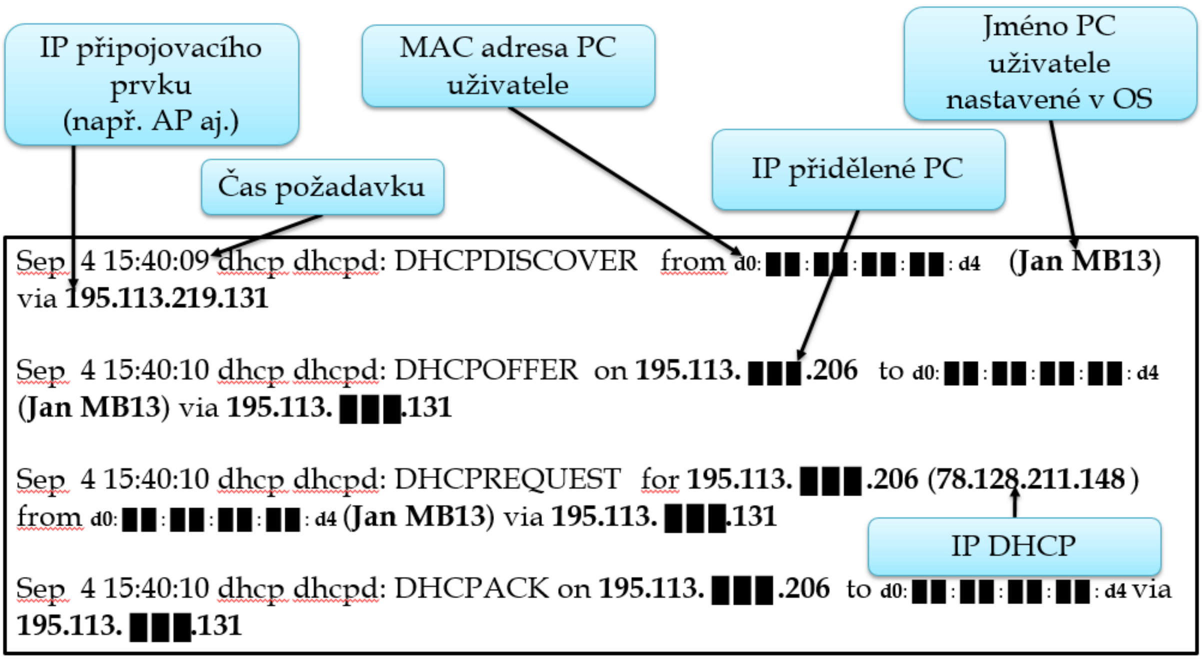


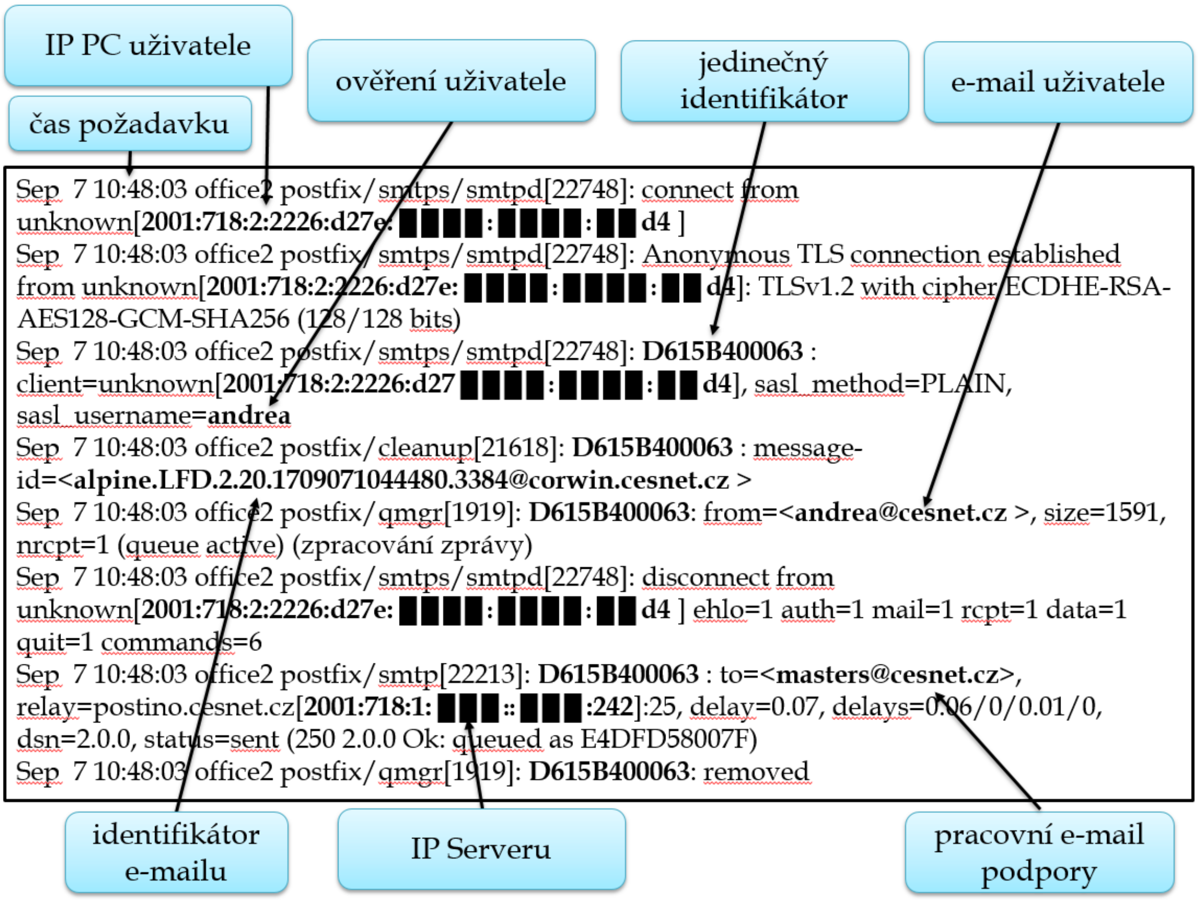
Figura: DHCP

IP připojovacího prvku (např. AP aj.)	IP do elemento de ligação (por exemplo, AP, etc.)
Čas pozadavku	Tempo de pedido
MAC adresa PC uzivatele	Endereço MAC do PC do utilizador
IP přidělené PC	IP atribuído ao PC
Jméno PC uzivatele nastavené v OS	O nome do PC do utilizador definido no SO
IP DHCP	DHCP IP

Se nos concentrarmos consistentemente em **dados** (informação) **que estejam relacionados com o sujeito dos dados e que sejam capazes de o identificar**, então os dados pessoais neste caso não serão apenas o endereço IP do elemento de ligação e o endereço IP do servidor DHCP.

Teoricamente, o momento de um pedido é também um dado pessoal, pois é um vestígio que pode ser utilizado para identificar uma pessoa singular, especialmente em combinação com identificadores únicos e outras informações que os servidores obtêm.[164] Ao mesmo tempo, esta informação é muito importante porque sem uma hora exacta não é possível identificar a quem (a que sistema informático) foi atribuído um endereço IP específico.

Outro exemplo que mostra a extensão do tratamento de dados que pode ser considerado como dados pessoais é o tratamento de dados pessoais quando se envia correio electrónico via SMTP.



IP PC uzivatele	Endereço IP do PC de um utilizador
čas požadavavku	tempo de pedido
ověření uzivatele	autenticação do utilizador
jedinečný identifickátor	identificador único
e-mail uzivatele	e-mail do utilizador
(zpracování zprávy)	(processamento de mensagens)
identifickátor e-mailu	identificador de e-mail
IP Serveru	Servidor IP
podpory de e-mail practiceovní	e-mail de trabalho de apoio

Figura: SMTP

Se voltarmos a concentrar-nos consistentemente nos **dados** (informação) **que estão relacionados com o sujeito dos dados e que são capazes de o identificar**, então os dados pessoais neste caso não serão apenas o endereço IP do elemento de ligação e o endereço IP do servidor DHCP.

[164] Para mais detalhes ver o considerando 30 do GDPR

O e-mail de trabalho de apoio poderá ser novamente dados pessoais se lhe forem atribuídos identificadores adicionais que sejam capazes de identificar uma pessoa singular.

A questão-chave é se, em todos os processos que têm lugar em sistemas informáticos (elementos TIC) que são geridos por uma entidade (pessoa singular ou colectiva), **somos capazes de distinguir uma situação em que os dados são transferidos unicamente entre sistemas informáticos sem relação com qualquer pessoa singular e quando a pessoa singular já estará envolvida nestes processos como sujeito de dados de acordo com o GDPR.**

Acreditamos que, com excepções específicas, não seremos capazes de destacar processos que ocorrem sem interacção humana. Com base nesta afirmação, os requisitos da GDPR deverão então ser aplicados a todos os processos que envolvam a manipulação de informação que seja relevante para o sujeito dos dados e capaz de o identificar. Ao mesmo tempo, será necessário tomar medidas de segurança suficientes para proteger suficientemente tanto o sistema de transmissão, como os sistemas informáticos e as aplicações que funcionam com tais informações e as próprias informações (ou dados).

Para além dos dados pessoais acima referidos, a GDPR define categorias específicas de dados pessoais que incluem dados sobre:

- origem racial ou étnica,
- religião,
- pontos de vista políticos,
- filiação em sindicatos ou outras organizações,
- orientação sexual,
- cometer delitos (crime/ordenacional, etc.) e puni-los,
- dados genéticos (ADN e ARN),
- dados biométricos,
- dados de saúde.

6.2.3 Tratamento de dados pessoais

Nos termos do n.º 2 do artigo 4º da GDRP, entende-se por tratamento de dados pessoais **qualquer operação** ou conjunto de operações efectuadas sobre **dados pessoais** ou sobre conjuntos de dados pessoais, com **ou sem meios automatizados, tais como** recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

A protecção da pessoa em causa aplica-se ao tratamento de dados pessoais quando tais dados são armazenados ou inscritos num registo.[165]

Contudo, de acordo com a GDPR, o **processamento não pode ser entendido como qualquer tratamento de dados pessoais. O tratamento de dados pessoais deve ser considerado como uma actividade mais sofisticada que um controlador realiza com dados pessoais para um determinado fim e fá-lo sistematicamente de um determinado ponto de vista .** [166]

---

[165] Ver o considerando 15 do GDPR

[166] Para mais detalhes ver *Základní příručka k GDPR.* [online]. [cit. 07/08/2018]. Disponível a partir de: *https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938*

Entre outras coisas, as **actividades realizadas por uma pessoa singular no âmbito de uma natureza puramente pessoal ou actividades realizadas exclusivamente num agregado familiar, e portanto sem qualquer ligação com actividades profissionais ou empresariais, são excluídas** do tratamento de dados pessoais de acordo com a GDPR. [167]

O artigo 5 (1) (a) do GDPR estabelece os princípios para o tratamento de dados pessoais. De acordo com o GDPR, estes princípios incluem:

- **legalidade, equidade e transparência** [Art. 5 (1) (a) do GDPR] - um controlador de dados pessoais é obrigado a fazê-lo:
    - informar a pessoa em causa sobre a operação de tratamento em curso e os seus objectivos,
    - informar o sujeito dos dados sobre a definição de perfis e suas consequências,
    - informar a pessoa em causa, se lhe forem obtidos dados pessoais, se esta é obrigada a fornecer esses dados e sobre as consequências da sua eventual não prestação,
    - **provar a existência de pelo menos uma razão legal para o tratamento de dados pessoais**,
    - **documento:**
        - o quê, como, porque é que processa,
        - consentimento e razão legal,
        - o tempo para o qual processa,
        - **garantias e medidas de segurança tomadas**.
- **limitação da finalidade** [Art. 5 (1) (b) da GDPR] - os dados pessoais devem ser recolhidos para fins específicos, explícitos e legítimos e não ser posteriormente processados de forma incompatível com esses fins,
- **minimização dos dados** [Art. 5 (1) (c) do GDPR] - os dados pessoais devem ser proporcionais e relevantes para o fim para o qual são processados,
- **exactidão** [Art. 5 (1) (d) da GDPR] - os dados pessoais devem ser exactos e, se necessário, actualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados pessoais inexactos em relação às finalidades para as quais são processados sejam apagados ou rectificados sem demora,
- **limitação de armazenamento** [Art. 5 (1) (e) do GDPR] - os dados pessoais devem ser mantidos numa forma que permita a identificação das pessoas em causa por um período não superior ao necessário para os fins para os quais são tratados,
- **integridade e confidencialidade** [Art. 5 (1) (f) da GDPR] - os dados pessoais devem ser **tratados de forma a garantir a segurança adequada dos dados pessoais, incluindo a protecção contra o processamento não autorizado ou ilegal e contra a perda, destruição ou danos acidentais, utilizando medidas técnicas ou organizacionais adequadas.**

6.2.4 Segurança dos dados pessoais

Uma das áreas que a GDPR aborda explicitamente é a **questão da segurança do processamento de dados pessoais**.

[167] Ver o considerando 15 do GDPR

O artigo 32 da GDPR estabelece que, tendo em conta o estado da técnica, os custos de implementação e a natureza, âmbito, contexto e objectivos do processamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o **controlador** (ou processador) **deve implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco**, incluindo, entre outros aspectos, conforme adequado:

- **a pseudonimização e encriptação de dados pessoais,**
- **a capacidade de assegurar a permanente confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de processamento,**
- **a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico,**
- **um processo para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento.**

"Na avaliação do nível de segurança adequado, devem ser tidos em conta, nomeadamente, os riscos *que o processamento apresenta, nomeadamente de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outro modo processados".*[168]

Ao determinar o risco, é necessário ter especialmente em conta a categoria de dados pessoais que podem ser afectados pela violação da segurança, a natureza da violação da segurança e o número de pessoas em causa. Os dados pessoais "mais sensíveis" (ver, por exemplo, categorias especiais de dados pessoais), um conjunto maior de dados pessoais, ou dados que possam causar danos à pessoa em causa ou interferir com os seus direitos, representam um risco mais elevado.

Nos termos do nº 4 do artigo 32º da GDPR, o responsável pelo tratamento e o subcontratante devem tomar medidas para assegurar que qualquer pessoa singular que actue sob a autoridade do responsável pelo tratamento ou do subcontratante que tenha acesso aos dados pessoais não os trate, excepto mediante instruções do responsável pelo tratamento, a menos que tal lhe seja exigido pela legislação da União Europeia ou dos Estados-Membros.

6.2.5 Avaliação do impacto da protecção de dados (DPIA)

A Avaliação de Impacto da Protecção de Dados (**DPIA**) é um instrumento a ser utilizado quando um determinado tipo de **tratamento é provável**, **especialmente quando se utilizam novas tecnologias**, tendo em conta a natureza, âmbito, contexto e finalidades do tratamento, o **que resulta num elevado risco para os direitos e liberdades dos indivíduos.** É um instrumento que pode ajudar os responsáveis pelo tratamento a identificar riscos potenciais do tratamento de dados pessoais e a implementar medidas adequadas.

Deve ser realizada uma avaliação do impacto da protecção de dados nos seguintes casos:

- uma **avaliação sistemática e abrangente dos aspectos pessoais relacionados com pessoas singulares, com base no processamento automatizado, incluindo o perfil** que determina decisões que produzem efeitos legais em relação a pessoas singulares ou que têm um impacto igualmente grave sobre pessoas singulares,
- **tratamento de categorias especiais de dados pessoais** (dados biométricos ou dados sobre condenações penais e sobre infracções penais ou medidas de segurança conexas),
- controlo sistemático extensivo de instalações acessíveis ao público,

[168] Artigo 32 (2) do PIBR

- **qualquer outra operação em que a autoridade de controlo competente considere que o tratamento é susceptível de constituir um risco elevado para os direitos e liberdades das pessoas em causa.**

A avaliação do impacto da protecção de dados deve incluir:

- descrição das operações de tratamento previstas,
- avaliação da necessidade e da adequação das operações em termos de finalidade (**teste de proporcionalidade**),
- **avaliação dos riscos para os direitos e liberdades das entidades**,
- **medidas planeadas para enfrentar estes riscos, incluindo garantias, medidas de segurança, etc.**

A própria GDPR também contém outras instituições (por exemplo, pseudonímia, requisitos de apagamento ou portabilidade de dados pessoais, etc.) que podem estar relacionadas com actividades realizadas no âmbito de sistemas de informação e comunicação e que requerem um nível adequado de segurança e protecção.

É importante identificar a influência (impacto) do GDPR sobre uma organização, sobre as suas partes e processos individuais. De facto, trata-se de uma auditoria em que, em toda a parte numa organização ou para o indivíduo, são processados dados pessoais em relação à GDPR. Subsequentemente, o procedimento baseia-se na modificação ou criação de regras e processos (se necessário) tanto dentro de uma organização como em relação à pessoa a quem os dados dizem respeito. Ao mesmo tempo, todas estas actividades devem respeitar os princípios básicos de segurança.

Tal como na implementação das regras de segurança em geral, ao implementar a GDPR ou outros documentos e recomendações, deve ter-se em mente que não existe uma regra, modelo, ferramenta, solução ou procedimento único aplicável a cada organização ou a cada situação.

É necessário adoptar e implementar a sua própria solução de acordo com o GDPR.

É necessário individualizar...

RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

- O GDPR é um quadro jurídico geral para a protecção de dados pessoais, e é válido e eficaz em toda a UE e, em certos casos, fora deste território. O principal objectivo da GDPR é assegurar uma protecção abrangente dos direitos das pessoas em causa contra o tratamento não autorizado dos seus dados e dados pessoais, encontrar um equilíbrio entre os interesses legítimos dos responsáveis pelo tratamento, dos processadores e das pessoas em causa, criar um sistema de aplicação uniforme da lei e um mecanismo único de sanções neste domínio, etc.
- No entanto, o GDPR aplica-se nos casos em que:
  - um controlador ou processador está estabelecido na UE, independentemente de o processamento ter lugar na UE,
  - os controladores ou processadores não estão estabelecidos na UE, mas
    - os bens ou serviços são oferecidos às pessoas em causa na UE (independentemente da remuneração),
    - a conduta das pessoas em causa dentro da UE é monitorizada.
- Nos termos do artigo 4 (1) da GDPR, os dados pessoais são "*qualquer informação relativa a uma pessoa singular identificada ou identificável". Uma pessoa singular identificável é aquela que pode ser identificada, directa ou indirectamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou a um ou mais factores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"*.
- Nos termos do n.º 2 do artigo 4º da GDRP, entende-se por tratamento de dados pessoais qualquer operação ou conjunto de operações efectuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, com ou sem meios automatizados, tais como recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.
- Tendo em conta o estado da técnica, os custos de implementação e a natureza, âmbito, contexto e objectivos do processamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o controlador (ou processador) deverá implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, incluindo, entre outros aspectos, conforme adequado:
  - a pseudonimização e encriptação de dados pessoais,
  - a capacidade de assegurar a permanente confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de processamento,
  - a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico,
  - um processo para testar, avaliar e avaliar regularmente a eficácia das medidas técnicas e organizacionais para garantir a segurança do processamento.
- A Avaliação de Impacto da Protecção de Dados (DPIA) é um instrumento a ser utilizado quando é provável que um determinado tipo de tratamento, especialmente quando se utilizam novas tecnologias, tendo em conta a natureza, âmbito, contexto e finalidades do tratamento,

resulte num elevado risco para os direitos e liberdades dos indivíduos. É um instrumento que pode ajudar os responsáveis pelo tratamento a identificar riscos potenciais do tratamento de dados pessoais e a implementar medidas adequadas.

PALAVRAS-CHAVE A LEMBRAR

- GDPR
- Dados pessoais
- Controlador de dados
- Tratamento de dados pessoais
- Avaliação do impacto da protecção de dados

PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- Qual é o âmbito territorial do GDPR?
- O que são dados pessoais em geral?
- Um endereço IP é um dado pessoal?
- Quais são as responsabilidades de um responsável pelo tratamento de dados pessoais?
- O que se entende por tratamento de dados pessoais?
- O que significa a Avaliação de Impacto sobre a Protecção de Dados?

7. Privacidade e segurança nas TIC, protecção de dados no ciberespaço

Viver na era digital com a ideia ou a sensação de que as minhas acções são anónimas ou escondidas dos olhos de outros utilizadores[169] é, na minha opinião, ingénuo. Com o advento da era digital, aparecem não só os seus aspectos positivos mas também os seus aspectos negativos.[170] Um desses aspectos negativos é o facto de estarmos cada vez menos interessados na essência do funcionamento dos serviços prestados no ciberespaço.

O nosso mundo, que cada vez mais entendemos como o "mundo da informação" ou "mundo da Internet", está firmemente ligado às tecnologias de informação e comunicação que interferem na vida de um indivíduo de uma forma muito significativa. Estas tecnologias facilitam o acesso à informação e simplificam ou aceleram a comunicação mútua entre utilizadores individuais, etc. Por outro lado, é importante perceber que qualquer publicação de informação da nossa vida privada na Internet representa o risco de exploração por qualquer pessoa no ciberespaço.

Todas as aplicações, quer sejam utilizadas em qualquer sistema informático, serviços web[171] e especialmente meios de comunicação social,[172] recolhem uma quantidade considerável de informação sobre os seus utilizadores. Não precisam desta informação para o seu funcionamento, mas permite tanto ao ISP em questão fornecer um serviço "gratuito" como "alvo" ou modificar os serviços que oferece. As informações que não são necessárias por defeito para a funcionalidade directa de serviços individuais incluem, por exemplo, informações de natureza **pessoal** (nome, apelido, endereço electrónico, número de telefone, endereço, etc.), natureza **sensível** (por exemplo, informações sobre o sistema operativo do computador utilizado, versões de aplicações individuais, cookies, etc.), **dados de localização** (coordenadas GPS, informações sobre Wi-Fi, GPRS, etc.), dados operacionais, etc. [173]

A informação pode ser utilizada de várias maneiras. De acordo com a informação, um prestador de serviços pode oferecer, por exemplo, serviços adicionais ou publicidade com base nos requisitos, interesses ou hobbies dos utilizadores. Graças a eles, a polícia pode criar um enquadramento para as actividades diárias de uma pessoa que, por exemplo, se perca ou seja raptada e assim agilizar as suas próprias actividades na busca dessa pessoa. Ao mesmo tempo, porém, a informação pode muito facilmente ser mal utilizada pelos criminosos, quer para estabelecer contacto com uma vítima, quer para planear um crime.

Ao fornecer (mesmo que involuntariamente ou involuntariamente) os dados, o utilizador do serviço permite que outras pessoas obtenham informações importantes sobre as suas vidas (por exemplo, informações sobre o seu comportamento durante o dia, locais visitados, actividades e pessoas com as

---

[169] O termo utilizador inclui todas as entidades que influenciam eventos no ciberespaço. É principalmente necessário incluir **os ISPs** neste grupo. Contudo, nem todos os PSIs estão sob a jurisdição da lei checa (quer por razões de geolocalização, quer porque as suas actividades não são reguladas pela lei). Outros "utilizadores" serão sem dúvida **LEAs** (Agências de Aplicação da Lei - que são autorizadas pelas normas de cada país a ser uma das intervenções mais intensivas em matéria de direitos humanos e liberdades fundamentais), **equipas CERT/CSIRT**, **administradores de TI**, **utilizadores finais, etc.**

[170] Por exemplo, cibercriminalidade, vícios e, entre outras coisas, a chamada demência digital. Para mais pormenores, ver: SPITZER, Manfred. *Digitátlní demência.* Brno: Host, 2014. ISBN 978-80-7294-872-7

[171] Ver por exemplo, *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají moňost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit.04/04/2014]. Disponível a partir de: https://www.google.cz/intl/cs/policies/?fg=1

[172] Ver *Prohlášení o právech a povinnostech.* [online]. [cit.04/04/2014]. Disponível em: https://www.facebook.com/legal/terms

[173] **No entanto, alguns sistemas de autenticação também precisam desta informação adicional para funcionar.**

quais está em contacto).[174] Neste ponto, **nós próprios tornamo-nos informação ou uma mercadoria com a qual outra pessoa pode negociar**.

Várias estatísticas disponíveis[175] indicam que a população total é actualmente de aproximadamente 7.359.244.000 pessoas. Deste número, cerca de 3,6 mil milhões de pessoas são utilizadores activos da Internet, e mais de 2,1 mil milhões de pessoas são utilizadores activos das redes sociais. Os dispositivos móveis são propriedade de mais de 3,6 mil milhões de utilizadores, e mais de 1,7 mil milhões de utilizadores ligam-se aos meios de comunicação social através destes dispositivos. As redes sociais são dominadas pelo Facebook, com mais de 1,59 mil milhões de utilizadores: [176]

Nesta secção, tentarei chamar a atenção para possíveis ameaças à segurança que estamos habituados a aceitar ou não perceber de facto e nas quais a maioria dos indivíduos ou organizações nem sequer estão conscientes do possível perigo.

7.1 Pegada digital

As ameaças mencionadas, ou melhor, os riscos, consistem muito frequentemente em deixar pegadas digitais no ciberespaço. As pegadas digitais, com base na possibilidade ou não de serem influenciadas por um utilizador, podem geralmente ser **divididas em pegadas que podem ser influenciadas (activas) e que não podem (passivas).**

Divisão de pegadas digitais:

- **Pegada digital passiva**
  - Informação de um sistema informático;
  - ligação a redes informáticas, em particular a Internet;
  - utilização dos serviços fornecidos, etc.
- **Pegada digital activa**
  - utilização consciente dos serviços;
  - divulgação voluntária de informação;
    - blogs, fóruns;
    - meios de comunicação social;
    - e-mail;
    - armazenamento de dados;

[174] KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN e Terezie JANÍKOVÁ. neBezpečné chování na Facebooku. In: *Sborník příspěvků ke konferenci: Sociální sítě. Mobilní aplikace.* Plzeň: Západočeská univerzita v Plzni, 2014, pp. 39-47. ISBN 978-80-261-0362-2 p. 40

[175] Para mais detalhes, ver, por exemplo
World Internet Users and 2015 Population Stats. [em linha]. [cit.09/08/2015]. Disponível em: http://www.internetworldstats.com/stats.htm
Digital, Social & Mobile Worldwide em 2015. [online]. [cit.09/08/2015]. Disponível a partir de: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/
Největší sociální sítě na světě? Facebook je sice jednička, ale... [online]. [cit.10/08/2015]. Disponível em: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/
População mundial actual. [em linha]. [cit.10/08/2015]. Disponível em: http://www.worldometers.info/world-population/

[176] *Redes sociais líderes a nível mundial a partir de Abril de 2016, classificadas por número de utilizadores activos (em milhões)* [online]. [cit.10/08/2015]. Disponível em: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

- serviços de nuvem, etc.

Na secção seguinte, centrar-me-ei em alguns aspectos das pegadas digitais individuais e da informação nelas contida. O objectivo é alertar os utilizadores de que as suas acções no ambiente dos sistemas de informação e comunicação não são tão anónimas como eles possam pensar.

No mundo das TIC, aplica-se uma regra: **sempre que carrega, transfere, medeia ou coloca algo no ciberespaço, ele fica lá "para sempre".** Haverá sempre uma cópia (criada com base na funcionalidade de um sistema informático ou uma cópia armazenada por outro utilizador) dos seus dados. E mesmo se posteriormente apagar os dados, estes não serão apagados de facto, permanente e irreversivelmente. Por conseguinte, é conveniente prestar atenção à sua pegada digital e às informações ou dados que deixamos para trás no ambiente do ciberespaço.

7.1.1 Pegada digital passiva

As pegadas passivas surgem mais frequentemente da interacção de um sistema informático com outro sistema informático ou da funcionalidade de um sistema informático (e software associado). Exemplos de tais pegadas podem ser informações do sistema operacional (tais como mensagens de erro do Windows ou informações do sistema), ou outras informações e dados que são armazenados com base na funcionalidade do sistema sem terem de ser transmitidos (tais como um sistema informático que nunca tenha sido ligado a qualquer rede ou outro sistema informático).[177] Dizer de forma totalmente intransigente que estas pegadas não podem ser influenciadas não seria inteiramente correcto. Se um utilizador tiver experiência suficiente, é capaz de alterar, mascarar ou suprimir uma série de pegadas digitais "passivas" (por exemplo, através de um simples modo anónimo do navegador da web que desliga os cookies). No entanto, o movimento de um utilizador na Internet pode ser monitorizado de várias maneiras.

Endereço IP

A ligação de um sistema informático à Internet é um exemplo típico de uma pegada relativamente passiva. Um endereço IP ou endereço MAC que são transmitidos juntamente com outras informações do ISP. Um endereço IP não é anónimo por defeito, e o sistema informático utiliza-o como um dos identificadores quando comunica com outros sistemas informáticos. Os endereços IP são atribuídos hierarquicamente, com a **ICANN a** desempenhar um papel dominante, dividindo o mundo real em regiões geridas por registadores regionais da Internet (**RIR** - **Regional Internet Registry**). A estes agentes de registo foi atribuída uma gama de endereços IP da ICANN, que atribuem aos LIRs dentro da sua região. Os agentes de registo regionais estão divididos nos cinco territórios seguintes:

1. Região "Euro-Asiática" - RIPE NCC: https://www.ripe.net/
2. Região "Ásia Pacífico" - APNIC: https://www.apnic.net/
3. Região "norte-americana" - ARIN: https://www.arin.net/
4. Região "América do Sul" - LACNIC: http://www.lacnic.net/
5. Região "africana" - AFRINIC: http://www.afrinic.net/

[177] Isto significa principalmente informação que é registada e arquivada sobre as actividades dos utilizadores em locais aos quais um utilizador não tem acesso e não as tem sob controlo [por exemplo, o utilizador não é capaz de apagar registos que provem a sua actividade (por exemplo, acesso, envio de correio electrónico, etc.) no servidor de correio]. No seu próprio computador, os utilizadores podem influenciar os dados e informações armazenados. Têm o direito de apagar (por exemplo, histórico, correio electrónico, etc.), editar, etc.

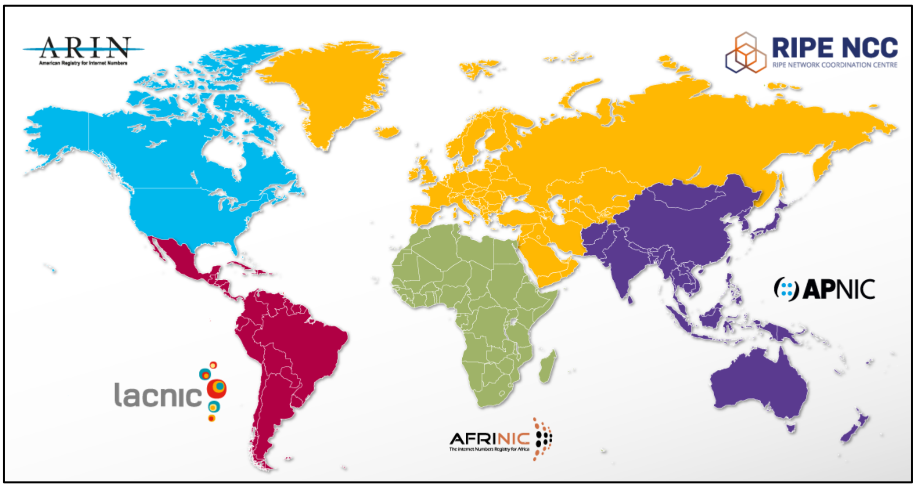
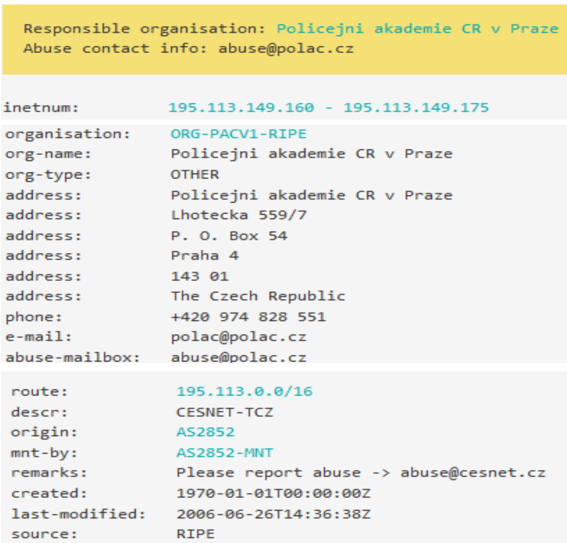


Figura - Divisão do mundo entre os RIRs

Os registadores regionais[178] exploram o serviço *Whois* nos seus sítios web, que é um nome para uma base de dados na qual estão registados dados sobre detentores de endereços IP. Estas bases de dados contêm uma vasta gama de informações que permitem a identificação, por exemplo, de uma série de endereços IP públicos utilizados, informações de contacto, contacto de abuso[179] , fornecedor de ligação hierarquicamente superior, etc. Para determinar um "proprietário" (operador, fornecedor) de um determinado endereço IP, é muitas vezes possível utilizar estas bases de dados livremente disponíveis. [180]



```
Responsible organisation: Policejni akademie CR v Praze
Abuse contact info: abuse@polac.cz

inetnum:        195.113.149.160 - 195.113.149.175

organisation:   ORG-PACV1-RIPE
org-name:       Policejni akademie CR v Praze
org-type:       OTHER
address:        Policejni akademie CR v Praze
address:        Lhotecka 559/7
address:        P. O. Box 54
address:        Praha 4
address:        143 01
address:        The Czech Republic
phone:          +420 974 828 551
e-mail:         polac@polac.cz
abuse-mailbox:  abuse@polac.cz

route:          195.113.0.0/16
descr:          CESNET-TCZ
origin:         AS2852
mnt-by:         AS2852-MNT
remarks:        Please report abuse -> abuse@cesnet.cz
created:        1970-01-01T00:00:00Z
last-modified:  2006-06-26T14:36:38Z
source:         RIPE
```

Figura - Informação extraída da base de dados RIR

Os registadores regionais dividem ainda mais os intervalos de IP atribuídos entre os registadores locais da Internet (**Local Internet Registry - LIR**). Um registador local é normalmente um ISP (na República Checa, um fornecedor de serviços da sociedade da informação, especificamente um fornecedor de ligação, público ou não público). Este agente de registo pode então fornecer a sua gama de endereços IP a, por exemplo, partes da sua organização ou outras entidades.

A selecção abreviada da base de dados do RIR mostra o LIR (neste caso a associação CESNET, z. s. p. o., utilizando a gama de endereços IP: 195.113.0.0/16) e uma organização à qual o CESNET atribuiu parte dos endereços públicos [Academia de Polícia da República Checa com a gama de endereços IP 195.113.149.160 - 195.113.149.175]. A Academia de Polícia pode novamente distribuir estes endereços entre outras partes da organização (por exemplo, faculdades, laboratórios, ou outras sub-redes que gere)]. Dependendo do endereço IP e da hora exacta, é possível determinar um sistema informático específico com base na atribuição hierárquica de endereços. As informações sobre uma ligação de um sistema

[178] *Registos regionais da Internet.* [em linha]. [cit.04/08/2015]. Disponível em: https://*www.nro.net/about-the-nro/regional-internet-registries*

[179] Este é um contacto com o qual um utilizador pode entrar em contacto se for prejudicado por um determinado endereço IP ou gama de endereços (por exemplo, há um ciberataque sob a forma de spam, phishing, etc.). É o contacto mais próximo da fonte do ataque.

[180] No entanto, esta não é a única base de dados. Há uma série de serviços que oferecem a mesma informação. Mencionarei também outras bases de dados como exemplo: http://whois.domaintools.com/; https://www.whois.net/; http://www.nic.cz/whois/; https://whois.smartweb.cz/, etc.

informático final (fonte) a um sistema informático alvo (por exemplo, ligação de computador à Internet e apresentação da página web requerida) são armazenadas por ISPs individuais ao longo do caminho entre a fonte e o alvo.

Devido às regras estritas que definem a gestão de endereços IP e bases de dados RIR acessíveis ao público que contêm informações sobre os detentores de blocos de endereços individuais, é possível descobrir muito rapidamente a que rede pertence um determinado endereço IP e a quem opera a rede. Graças ao registo de informações do tráfego de rede, o operador de uma determinada rede é então capaz de identificar quem (ou que sistema informático) utilizou um determinado endereço IP num determinado momento. Esta determinação é uma fonte de informação muito importante no tratamento de incidentes de segurança (ciberataques) e na procura da sua fonte (originador).

Email

O e-mail, como um dos serviços mais frequentemente utilizados no ambiente da Internet, não é definitivamente um serviço anónimo. Uma mensagem que é enviada de uma fonte para um destino (destinatário) contém normalmente uma série de diferentes tipos de informação que podem identificar tanto o fornecedor do serviço (e-mail) como o fornecedor de ligação do dispositivo a partir do qual o e-mail foi enviado. Esta informação não é exibida no corpo da mensagem (ou seja, o texto que enviamos a uma pessoa específica) mas sim no código fonte (cabeçalho) da mensagem. A partir deste código fonte, é possível descobrir o caminho através de servidores, remetente real, nome do computador de origem, nome do computador, hora de envio da mensagem (incluindo fuso horário) utilizada pelo sistema operativo, cliente de correio, etc. Abaixo está um exemplo de um cabeçalho de correio electrónico fraudulento encaminhado[181] com informações potencialmente interessantes assinaladas.

```
From - Wed Aug 19 15:14:52 2015
X-Account-Key: account1
X-UIDL: 7
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Received: from relay.fit.cvut.cz (relay.fit.cvut.cz [147.32.232.237])
    by email-smtpd5.ko.seznam.cz (Seznam SMTPD 1.3.4) with ESMTP;
    Wed, 19 Aug 2015 15:14:16 +0200 (CEST)
Received: from imap.fit.cvut.cz (imap.fit.cvut.cz [IPv6:2001:718:2:2901:0:0:0:238])
    by relay.fit.cvut.cz (8.15.2/8.15.2) with ESMTP id t7JDE1Mm072888
    for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
Received: from PCP[redacted](cust-178.17.4.174.uvt.cz [178.17.4.174] (may be forged))
        (authenticated bits=0 as user ko[redacted])
        by imap.fit.cvut.cz (8.15.2/8.15.2) with ESMTPSA id t7JDE139012575
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
        for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
X-Authentication-Warning: imap.fit.cvut.cz: Host cust-178.17.4.174.uvt.cz [178.17.4.
From: "JUdr. Jan Kolouch, Ph.D." <jan.kolouch@fit.cvut.cz>
To: <kyber.test@seznam.cz>
References: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
In-Reply-To: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
Subject: =?UTF-8?Q?FW:_Chci=2C_aby_partner_s_v=C3=A1mi_na_?=
    =?UTF-8?Q?tomto_projektu?=
Date: Wed, 19 Aug 2015 15:14:15 +0200
Message-ID: <006901d0da80$f3599db0$da0cd910$@fit.cvut.cz>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_006A_01D0DA91.B6E2BBD0"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQDP5b3kQbONWI2VUUpIa1oprzeNE6AVNk1w
Content-Language: cs
X-FIT-MailScanner-ID: t7JDE1Mm072888
X-FIT-MailScanner: Found to be clean
X-FIT-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-0.381, required 7, autolearn=not spam, RP_MATCHES_RCVD -0.38)
X-FIT-MailScanner-From: jan.kolouch@fit.cvut.cz
X-FIT-MailScanner-Watermark: 1440594843.20583@MBoaO3F9jzMModBIjGdzYg
X-Spam-Status: No
```

Figura - Ver informação do cabeçalho de uma mensagem de correio electrónico

---

[181] o e-mail foi reencaminhado de: jan.kolouch@fit.cvut.cz para: kyber.test@seznam.cz

Navegador web

Um web browser é outra aplicação que por defeito passa informação sobre um utilizador e o seu sistema informático para o sistema informático (servidor) de um sítio visitado. Dentro de uma consulta de um cliente, este servidor descobre então, por exemplo, o referrer (que é a página de onde o utilizador vem), o navegador web utilizado e o sistema operativo (incluindo a versão exacta), cookies, flash cookies, histórico, cache, etc.

Para além do endereço IP, estes são, entre outras coisas, cookies[182] que ajudam a criar uma "impressão digital" do sistema informático do utilizador (computador, smartphone, etc.). Esta impressão digital permite a especificação de um sistema informático específico[183] , mesmo que o utilizador utilize um navegador web diferente, ou elimine cookies, inicie a sessão a partir de um endereço IP diferente, etc.

Uma das muitas formas de criar "impressões digitais" actualmente em uso é a recolha de impressões digitais em tela.[184] A recolha de impressões digitais em tela funciona através de um servidor web visitado que instrui o navegador web do utilizador a "desenhar uma imagem oculta". Esta imagem é exclusiva de qualquer navegador da web e sistema informático. A imagem desenhada é então convertida num código de identificação, que é armazenado no servidor web no caso de o utilizador a visitar novamente. [185]

Figura - Exemplo de Impressão Digital em Tela

Para além da recolha de impressões digitais, é também interessante monitorizar a transferência de informação para terceiros (tanto entidades como serviços que podem utilizar mais informação do utilizador) num navegador da web. Por defeito, esta transferência tem lugar com base nos Termos de Serviço acordados com um ISP. Por exemplo, cada utilizador final pode utilizar a aplicação Light Beam[186] , que exibe todas as páginas com as quais um utilizador (muitas vezes inconscientemente) comunica no sítio web. (Os dados são transmitidos a terceiros.) A transmissão de informação sobre os utilizadores a terceiros não é certamente excepcional. Pelo contrário, no mundo digital é uma questão natural e um "pré-requisito necessário" para o funcionamento de muitos ISPs.

1. O primeiro slide mostra a actividade do Firefox para o período de 30 de Julho de 2016 a 4 de Agosto de 2016. Durante esse período, foram visitadas 154 páginas, e 390 **páginas de terceiros** foram ligadas**.**

---

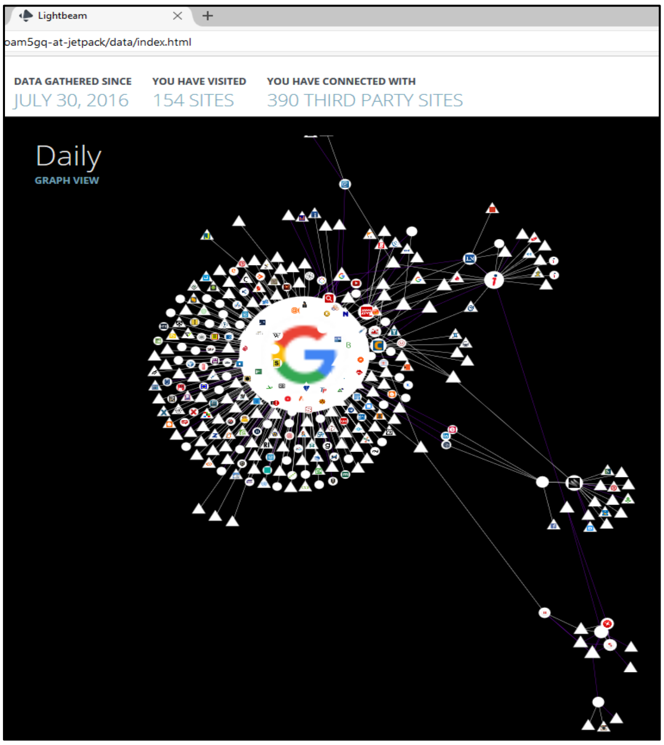
[182] Em HTTP, o termo cookie refere-se a uma pequena quantidade de dados que um servidor web visitado (uma página web visitada) envia para um navegador web, que depois os armazena no computador do utilizador. Estes dados são então enviados de volta para o servidor web cada vez que se visita o mesmo servidor.

[183] Se um utilizador quiser saber mais sobre o que um web browser revela sobre a sua actividade, recomendo os seguintes URLs: http://panopticlick.eff.org, http://browserspy.dk/, http://samy.pl/evercookie.

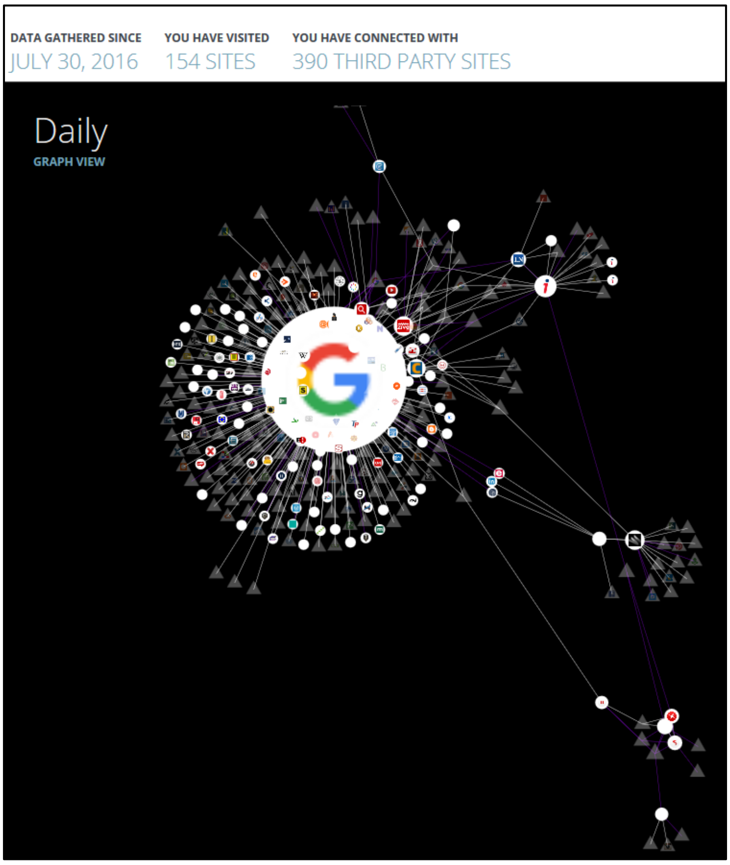
[184] ANGWIN, Julia. *Conheça o Dispositivo de Rastreio Online que é Virtualmente Impossível de bloquear.* [online]. [cit.10/06/2016]. Disponível em: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[185] Exemplo de recolha de impressões digitais em tela. Um teste que mostra a impressão digital do seu navegador pode ser testado dentro do artigo ANGWIN, Julia. *Conheça o Dispositivo de Rastreio Online que é Virtualmente Impossível de bloquear.* [online]. [cit.10/06/2016]. Disponível em: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

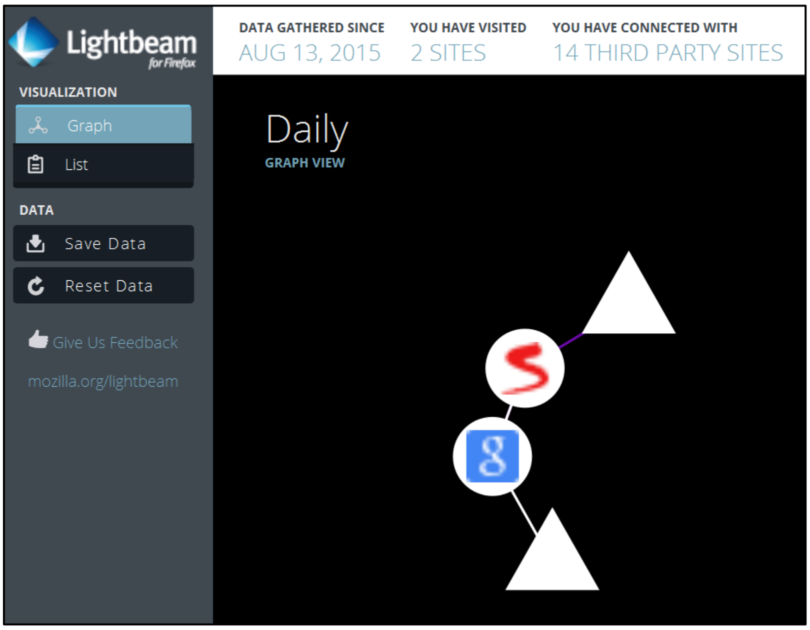
[186] A aplicação permite a visualização gráfica da interligação de serviços individuais e a transferência de informação para terceiros. Este é um add-on do navegador Firefox que está disponível em: https://www.mozilla.org/en-US/lightbeam/.



2. O segundo ecrã de impressão exibe o mesmo mapa mas filtra páginas de terceiros que são representadas por triângulos.



3. O último ecrã de impressão exibe a aplicação LightBeam após a limpeza e exibição das seguintes páginas: www.seznam.cz; www.google.com;



Outras aplicações

Na parte seguinte do texto, centrar-me-ei parcialmente nos dispositivos inteligentes (smartphones, tablets, etc.) e aplicações associadas a actividades de "dispositivos inteligentes". Escolho propositadamente estes dispositivos porque são sistemas informáticos nos quais os utilizadores instalam provavelmente o maior número de programas (muito frequentemente não verificados, apenas recomendados por um "amigo"). São estes dispositivos que, devido aos termos e condições contratuais, entre outras coisas, não têm de estar sob o controlo total do utilizador, administrador, etc., que representam um risco de segurança tanto para o utilizador final como para a empresa (organização).

O inquérito estatístico anteriormente mencionado[187] mostra que, em média, gastamos na Internet: 4,4 horas (acesso via computador sob a forma de um computador de secretária ou portátil, etc.) e 2,7 horas (acesso via dispositivos móveis) por dia. No caso de um computador, a segurança do dispositivo é geralmente garantida, mas os dispositivos móveis (smartphones, tablets, etc.) normalmente não têm políticas definidas para uma possível instalação de software (seja de fontes confiáveis ou não confiáveis) e muitas vezes carecem de protecção básica sob a forma de um programa antivírus.[188]

---

[187] *Digital, Social & Mobile Worldwide em 2015.* [online]. [cit.09/08/2015]. Disponível a partir de: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

[188] Deve notar-se que, por exemplo, um relatório emitido pela Kaspersky Lab mostra que existem mais de 340.000 tipos de malware destinados principalmente a dispositivos móveis. A Kaspersky Lab afirma ainda que 99% deste malware visa os dispositivos Android. Deve notar-se que este alvo é perfeitamente compreensível uma vez que a variabilidade de dispositivos individuais e versões do SO Android é considerável. (Alguns relatórios afirmam que mais de 24.000 tipos de dispositivos diferentes utilizam o sistema operativo Android).
Para mais detalhes, ver, por exemplo
O primeiro malware móvel: como Kaspersky Lab descobriu Cabir. [online]. [cit.01/08/2016]. Disponível a partir de: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
Ver também: *Estatísticas interessantes sobre Estratégias Móveis para Transformações Digitais.* [online]. [cit.15/07/2016]. Disponível em: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/
A fragmentação do Android tem novos registos: 24 000 dispositivos diferentes. [em linha]. [cit.15/07/2016]. Disponível a partir de: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

Um utilizador final tem a opção de instalar principalmente software no dispositivo do SO Android, e este software irá transmitir (a outras entidades) e armazenar informação sobre as suas actividades, incluindo o armazenamento e transferência do conteúdo da informação transmitida. O serviço Play Store, que é fornecido pela Google dentro do SO Android, permite a qualquer desenvolvedor definir regras para o que a aplicação deve recolher, por exemplo, e para onde enviar esses dados.

Pessoalmente, acredito que não é um erro permitir aos criadores e desenvolvedores de aplicações obter informação suficiente sobre as suas aplicações, a sua funcionalidade, etc. Se regularmos a recolha desta informação, então iremos sem dúvida regular e dificultar o possível progresso e subsequente desenvolvimento destas e de outras aplicações. Por outro lado, há atacantes que, porque a Play Store não autentica e escaneia aplicações, podem oferecer aplicações infectadas por malware que, quando instaladas num sistema de computador final, podem assumir o controlo de um smartphone de utilizador final, por exemplo.

Identificação de um sistema informático baseado em informações dos seus componentes

Um dos identificadores únicos, mas em algumas circunstâncias variáveis, do sistema informático é um endereço MAC, que está fortemente ligado a um cartão de rede do sistema informático. Contudo, uma placa de rede não é o único componente de hardware capaz de transmitir um identificador único de sistema informático a outro sistema informático.

Os investigadores da Universidade de Princeton descobriram que um sistema informático pode ser identificado, por exemplo, pela informação da bateria do sistema, e os navegadores da Web são uma parte essencial da transmissão desta informação. [189]

Na prática, é utilizado um procedimento que utiliza as capacidades do HTML5. Esta norma inclui uma função que permite aos sítios web (ou servidores web) identificar um nível de bateria do sistema informático que lhes acede. (A informação é transmitida sobre qual a percentagem da bateria restante e quanto tempo aproximadamente demora a descarregar ou carregar). A ideia dos proprietários de servidores web é que um utilizador que esteja a ficar sem bateria será mostrado uma versão rentável de uma página web. Os dois guiões descritos pelos investigadores da Universidade de Princeton já estão de facto a utilizar dados sobre a bateria, ao mesmo tempo que recolhem informação adicional - tal como um endereço IP ou uma impressão digital em tela. Tais combinações já podem fornecer uma identificação muito precisa de um sistema informático.[190]

7.1.2 Pegada digital activa

Uma pegada digital activa que pode ser influenciada representa toda a informação que um utilizador transfere voluntariamente sobre si próprio para outra pessoa (quer seja natural ou legal, ou mesmo ISP). A transferência pode incluir uma série de actividades, tais como o envio de um correio electrónico, adição de um post a uma discussão, fórum, publicação de qualquer meio de comunicação (foto, vídeo, áudio, etc.) em meios de comunicação social, etc. O termo também inclui um registo e utilização de todos os serviços concebíveis no ciberespaço [por exemplo, sistemas operacionais, e-mails (incluindo freemail), redes sociais, encontros, redes P2P, chats, blogs, quadros de avisos, websites, serviços de nuvem, armazenamento de dados, etc.].

As pegadas digitais activas são pegadas sobre as quais os utilizadores podem ter relativo controlo, e só a eles cabe a informação sobre si próprios que pretendem colocar à disposição dos outros. No

[189] Para mais detalhes ver ENGLEHARDT, Steven e Ardvin NARAYANANAN. *Acompanhamento online: Uma medição e análise de 1 milhão de sítios.* [online]. [cit.05/08/2016]. Disponível a partir de: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[190] Para mais detalhes ver VO'ENÍLEK, David. *Promazání "sušenek" nepomůže, na internetu vás prozradí i baterie.* [online]. [cit.04/08/2016]. Disponível a partir de: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

entanto, é necessário chamar a atenção para a premissa já mencionada: quaisquer dados ou informações introduzidas no ciberespaço permanecerão no ciberespaço.

Teoricamente, seria possível definir uma categoria de **pegadas hipotéticamente activas**, que é de certa forma um oxímoro. No entanto, esta categoria inclui determinados factos que um utilizador pode teoricamente influenciar, ou seja, é capaz de os influenciar, mas normalmente não o faz porque, de facto, limitaria significativamente o seu funcionamento no mundo digital. Estas pegadas poderiam incluir, por exemplo, a utilização dos serviços dos maiores ISPs (Microsoft, Apple, Google, Facebook, etc.), para os quais a utilização do serviço está sujeita ao acordo dos Termos de Serviço (EULA) que, por sua vez, permitem a estes ISPs obter uma quantidade significativa de informação. Além disso, é possível incluir nestas pegadas também pegadas que surgiram, por exemplo, através da correlação de pegadas activas e passivas; informação que outros utilizadores revelam sobre nós; dados que são espelhados; dados EXIF.[191]

7.2 Termos de Serviço (EULA)

Na próxima parte deste capítulo, tentarei descrever que informação sobre os utilizadores é recolhida por defeito pelos maiores ISPs.[192] Escolhi especificamente a Google Inc. porque acredito que existe um pequeno número de utilizadores que nunca utilizariam um dos produtos da Google (como o OS Android, o motor de busca em www.google.com, Gmail, Google Chrome, etc.).[193] O meu objectivo não é de forma alguma "atacar" a Google Inc. ou outras empresas (incluindo os seus produtos). O objectivo é apresentar os possíveis riscos de segurança associados à utilização de certos serviços fornecidos e à aceitação dos Termos de Serviço (EULA - End Users Licence Agreement), aos quais a utilização destes serviços está vinculada.

Os Termos de Serviço que permitem a utilização de um serviço de um determinado prestador de serviços não são, na essência, mais do que uma definição geralmente estabelecida unilateralmente de direitos e obrigações por parte do prestador de serviços (ISP). No entanto, um utilizador não está de modo algum limitado nos seus direitos, uma vez que tem a opção de não utilizar tais termos de serviço estabelecidos unilateralmente. No caso de consentimento para a utilização de tais serviços, é geralmente possível afirmar que as normas de direito privado serão aplicadas principalmente.

A questão é saber se um utilizador está realmente ciente dos Termos de Serviço com os quais concordou, quando estes se tornam vinculativos para ele e que possível interferência (legal) nos seus direitos humanos e liberdades fundamentais é tal consentimento. Outro facto importante é que o serviço prestado desta forma pode afectar os direitos e interesses legítimos (por exemplo, segurança informática, fiabilidade dos dados, etc.) de terceiros (por exemplo, empregadores, etc.) que não tenham concordado explicitamente em utilizar o serviço.

---

[191] EXIF - *Formato de ficheiro de imagem permutável*. É um formato de metadados que é incorporado em fotografias digitais por câmaras digitais. Estes metadados incluem, por exemplo:

- Marca e modelo da câmara.
- Data e hora em que foi tirada uma fotografia.
- Posição GPS.
- Informação sobre o autor (a pessoa que registou a câmara).
- Definições da câmara.
- Pré-visualização de uma imagem, etc.

[192] Para esta parte do texto, as teses que foram utilizadas foram publicadas no artigo: KOLOUCH, Jan. Pseudoanonymita - bezpečnostní riziko pro uzivatele Internetu. *DSM - gestão de segurança de dados* [online]. 2015. Vol. 19, No. 3, pp. 24-29 ISSN 1211-8737. Disponível em: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

[193] É de notar que as seguintes empresas têm Termos de Serviço muito semelhantes (permitindo-lhes fornecer informação numa medida comparável): Microsoft, Apple, Facebook, etc.

Teoricamente, pode afirmar-se que um contrato de direito privado com esta empresa para todo o período da sua existência foi celebrado por quase 3 mil milhões de utilizadores.[194] O triste facto é que uma percentagem muito pequena de utilizadores está disposta a ler os Termos de Serviço relativos a um serviço prestado.[195]

Excertos de Google Inc. Termos de Serviço[196]

O Google declara explicitamente que se algum utilizador começar a utilizar quaisquer serviços Google, concorda com os termos de serviço aplicáveis. Define ainda claramente a relação entre um utilizador e ele próprio, como fornecedor de serviços, caso o utilizador seja obrigado a aceitar outros termos de serviço. Esta relação é expressa da seguinte forma: *"A nossa gama de serviços é ampla, e alguns podem estar sujeitos a condições ou requisitos adicionais (incluindo restrições de idade).* ***Termos adicionais*** *estarão disponíveis juntamente com os serviços aplicáveis.* ***Se utilizar estes serviços, as condições de serviço adicionais tornam-se parte dos acordos contratuais entre as duas partes".***

Na introdução aos Termos de Serviço, o Google afirma que: ***"Podemos rever o conteúdo***[197] ***para determinar se é legal e em conformidade com as nossas políticas*** *e se acreditamos que viola as nossas políticas ou leis, podemos remover ou impedir que o conteúdo apareça. Note que o* ***acima exposto não significa que revejamos o conteúdo"***.

Do ponto de vista da segurança, na minha opinião, uma parte essencial dos Termos de Serviço é a secção que trata da **protecção dos dados pessoais e dos direitos de autor.**[198] Nesta secção, o Google define que informação recolhe sobre os utilizadores e como a trata. As seguintes informações são cruciais do ponto de vista da segurança e do "anonimato". Creio que declarar que a seguinte informação é recolhida *"para que possamos fornecer um melhor serviço a todos os nossos utilizadores - desde identificar coisas simples como a língua que fala até coisas mais complexas, tais como anúncios que lhe serão mais úteis, as pessoas que lhe interessam mais na web ou quais os vídeos do YouTube de que poderá gostar",* pode ser louvável mas pelo menos assustador. A comparação com o já mencionado *Relatório Minoritário sob a* forma de publicidade dirigida é mais do que óbvia após tal afirmação. Além disso, Manfred Spitzer e *Digital Dementia* vêm-me de novo à mente porque, com o tempo, já não sou eu quem decide o que vou ver ou o que vou procurar (ou todas as respostas relevantes podem não ser e não me são oferecidas).

O Google recolhe informação do utilizador basicamente de duas formas:

1. **Informação divulgada por um utilizador.** Normalmente, são estas:
   - *Nome, endereço de correio electrónico, número de telefone ou cartão de crédito.*
2. **Informação obtida através da utilização dos serviços Google.** Envolve a recolha de informação sobre os serviços que um utilizador utiliza, incluindo a forma como são utilizados (*"por exemplo,*

[194] De acordo com o artigo SMITH, Craig. *Pelos Números: 100 Fatos e Estatísticas de Pesquisa Incríveis no Google.* [online]. [cit. 04/08/2016]. Disponível em: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/, há 100 mil milhões de pesquisas por mês através da pesquisa no Google.

[195] E de acordo com um participante na conferência Security 2015, uma pessoa normal passaria cerca de 10-20 anos da sua vida a ler todos os Termos de Serviço em constante mudança.

[196] A seguir referido como o Google. Todos os excertos dos Termos de Serviço foram extraídos de: *Smluvní podmínky společnosti Google.* [online]. [cit.14/06/2016]. Disponível a partir de: https://www.google.cz/intl/cs/policies/terms/regional.html

[197] Conteúdo significa conteúdo (dados) que não pertence ao Google. A entidade que o publicou é responsável pelo conteúdo.

[198] Especificamente então *Zásady ochrany osobních údajů.* [online]. [cit.14/06/2016]. Disponível a partir de: https://www.google.cz/intl/cs/policies/privacy/

quando vê um vídeo no YouTube, visita websites que utilizam os nossos serviços de publicidade ou vê ou responde aos nossos anúncios e conteúdos"). De acordo com a Google, estes são:

- **Informação do dispositivo** *(por exemplo, modelo do hardware, versão do sistema operativo, identificadores únicos do dispositivo*[199] *e informação da rede móvel, incluindo o número de telefone).* Google reserva-se o direito de atribuir os identificadores do seu dispositivo ou o seu número de telefone à sua conta de utilizador Google
- ***Informação de protocolo:***
    - *detalhes de como um utilizador utilizou um serviço Google,*
    - *informação do protocolo de chamada (por exemplo, número de telefone, número de chamada, números de desvio, hora e data das chamadas, duração da chamada, dados de encaminhamento de SMS e tipos de chamadas),*
    - *Endereço do Protocolo Internet*
    - *informação sobre eventos do dispositivo (por exemplo, falha, actividade do sistema, definições de hardware, tipo de navegador, idioma do navegador, data e hora do seu pedido, ou URL de referência),*
    - *cookies, que podem ser identificadores únicos do seu browser ou da sua conta Google.*
- ***Informação sobre a localização.*** A Google pode recolher e processar mais informações sobre a localização real do seu utilizador. A Google pode determinar a sua localização utilizando uma variedade de tecnologias, tais como endereço IP, GPS e outros sensores que podem fornecer à Google informações sobre dispositivos próximos, hotspots Wi-Fi e transmissores de rede móvel.
- ***Números de candidatura únicos.*** **Normalmente, trata-se de um número e tipo de licença (versão) de um produto de software instalado aplicável.** Os Termos de Serviço não implicam que os números únicos de aplicação sejam registados apenas a partir de dispositivos cujo sistema operativo principal é o Android. Por conseguinte, pode concluir-se que, se forem utilizados serviços Google, a informação sobre números de aplicação únicos é também recolhida de outros sistemas operativos (iOS, Linux, Windows, etc.).
- ***Armazenamento local.*** **Nos termos dos Termos de Serviço, a Google pode**: *"recolher e armazenar informações (incluindo informações pessoais) no armazenamento local do seu dispositivo".* Também neste caso, pode-se chegar à mesma conclusão que para números de aplicação únicos.

  Na minha opinião, o problema é também o facto de em parte alguma dos Termos Gerais de Serviço estar definido com precisão[200] qual a localização e especialmente qual a segurança

---

[199] Definição do Google. *Identificador de dispositivo único.* [online]. [cit.14/06/2016]. Disponível em: https://www.google.cz/intl/cs/policies/privacy/key-terms/#toc-terms-unique-device-id
"Um identificador de dispositivo único (por vezes chamado um ID ou UUID universalmente único) é uma cadeia de caracteres que é codificado no dispositivo pelo fabricante e é utilizado para identificar de forma única o dispositivo (por exemplo, o IMEI de um telemóvel). Os diferentes identificadores de dispositivos diferem dependendo de serem permanentes, se os utilizadores podem reiniciá-los e como podem ser acedidos. Um determinado dispositivo pode conter vários identificadores únicos diferentes. Os identificadores únicos de dispositivos podem ser utilizados para uma variedade de fins, tais como segurança, detecção de fraude, sincronização de serviços, tais como caixa de entrada, ou para armazenar configurações de utilizadores e fornecer anúncios relevantes".

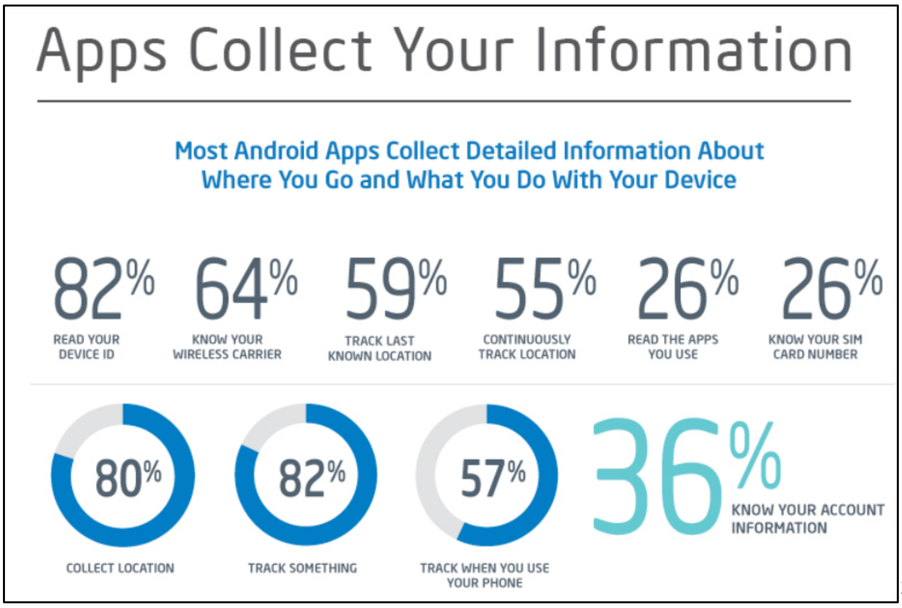
[200] De acordo com a função requerida, tratar-se-á principalmente de armazenar informações e dados na pasta do navegador (web browser) dado, mas de acordo com as condições contratuais, pode também ser aplicações diferentes de um web browser.

que será utilizada pelo Google. Assim, é teoricamente possível utilizar o armazenamento como um todo. É possível obter informações sobre ficheiros (por exemplo, os seus nomes, localização, e até absurdamente o hash, que será depois comparado, por exemplo, com a base de dados de outro serviço onde os dados são armazenados - por exemplo, DropBox, OneDrive, etc.).

Na minha opinião, a possibilidade de utilização abusiva de tais dados armazenados por um atacante é também uma ameaça para os utilizadores. A informação (que normalmente é embalada em cookies, etc.) armazenada no armazenamento local de um utilizador pode também tornar-se um alvo atraente para um atacante, porque é a partir desta informação que é possível determinar, por exemplo, os padrões de comportamento do utilizador.

- ***Biscoitos e tecnologias similares.*** *"Quando visita um serviço Google, nós e os* ***nossos parceiros*** *utilizamos uma variedade de tecnologias para recolher e armazenar informação. Isto pode incluir, mas não está limitado à utilização de cookies ou tecnologias semelhantes para identificar o seu navegador ou dispositivo. Utilizamos estas tecnologias para* ***recolher e armazenar informações, mesmo quando o utilizador utiliza serviços que oferecemos aos nossos parceiros****, tais como serviços de publicidade ou funcionalidades Google que possam aparecer noutros websites".*

Que informações recolhem as aplicações que correm no SO Android:



[201]

O Google pode continuar a utilizar esta informação com base nos Termos de Serviço acordados. Entre outras coisas, o Google está autorizado a analisar o conteúdo (incluindo e-mails) utilizando sistemas automatizados. Tem também o direito de combinar dados pessoais de um serviço com informações e dados pessoais de outro serviço (utilizando o Google).

O tratamento das informações mencionadas significa então a sua partilha, quer com o consentimento do utilizador, quer sem este consentimento.[202] O Serviço de Termos permite a **partilha para processamento externo e por razões legais**:

---

[201] CAETANO, Lianne. *As suas aplicações estão a ser sobre-partilhadas? O Relatório de Segurança Móvel de 2014 diz tudo.* [online]. [cit.10/04/2015]. Disponível a partir de: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

[202] Por exemplo, com administradores de domínio; para processamento externo ou por razões legais.

"Fornecemos informações pessoais aos nossos afiliados ou outras empresas ou pessoas de confiança para que as processem por nós, com base nas nossas instruções e em conformidade com a nossa Política de Privacidade e quaisquer outras medidas de confidencialidade e segurança apropriadas.

"Partilhamos informação pessoal com empresas, organizações ou indivíduos** fora do Google **se acreditarmos de boa fé que o acesso, utilização, preservação, ou divulgação da informação é razoavelmente necessário:

- *cumprir qualquer lei aplicável, regulamento, processo legal, ou pedido governamental executório,*
- *fazer cumprir os Termos de Serviço aplicáveis, incluindo a investigação de potenciais violações,*
- *detectar, prevenir, ou de outra forma abordar a fraude, segurança, ou questões técnicas,*
- *proteger contra danos aos direitos, propriedade ou segurança da Google, dos nossos utilizadores, ou do público, conforme exigido ou permitido por lei".*

No entanto, de uma perspectiva de segurança e anonimato, considero a seguinte secção dos Termos de Serviço que trata do conteúdo do utilizador sobre os serviços fornecidos pelo Google como provavelmente a mais problemática:

*"Ao **carregar, submeter, armazenar ou receber conteúdo para ou através dos nossos Serviços, concede à Google** (e aos seus parceiros) **uma licença mundial para utilizar, alojar, armazenar, reproduzir, modificar, criar trabalhos derivados** (por exemplo, os que são da tradução, adaptação ou outras alterações que fazemos para que o seu conteúdo se adapte melhor aos nossos Serviços)*[203] *, **comunicar, publicar, executar ou exibir e distribuir publicamente o referido conteúdo.....** Esta licença permanecerá em vigor mesmo quando deixar de utilizar os nossos Serviços (por exemplo, listagem de empresas adicionadas ao Google Maps). **Alguns serviços permitem-lhe aceder ou remover conteúdo que tenha submetido ao serviço....** "*

Pessoalmente, acredito que pelo menos nesta parte dos Termos de Serviço, o limite imaginário que define a adequação da informação recolhida sobre utilizadores individuais foi excedido. Esta secção é, de facto, sobre uma "utilização legal" de qualquer conteúdo com o qual o Google "interage". Pessoalmente, acredito que é a interferência com o conteúdo de, por exemplo, informação transmitida que deveria ser um último recurso possível, e não uma espécie de "assunto em curso" consagrado no contrato.

[203] É compreensível que o Google tente, por exemplo, traduzir obras, páginas ou outros conteúdos para que mesmo um utilizador que não conheça a língua original da obra o possa ler. No entanto, em casos absurdos, é possível imaginar a publicação do seu poema de amor privado que enviou utilizando um dos serviços Google, a sua fotografia, a sua brilhante ideia de uma máquina de movimento perpétuo, etc.

RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

- Todas as aplicações, quer sejam utilizadas em qualquer sistema informático, serviços web e especialmente nas redes sociais, recolhem uma quantidade considerável de informação sobre os seus utilizadores. Não precisam desta informação para o seu funcionamento, mas permite tanto ao ISP em questão fornecer um serviço "gratuito" como "alvo" ou modificar os serviços que oferece. As informações que não são necessárias por defeito para a funcionalidade directa de serviços individuais incluem, por exemplo, informações de natureza pessoal (nome, apelido, endereço electrónico, número de telefone, endereço, etc.), natureza sensível (por exemplo, informações sobre o sistema operativo do computador utilizado, versões de aplicações individuais, cookies, etc.), dados de localização (coordenadas GPS, informações sobre Wi-Fi, GPRS, etc.), dados operacionais, etc.
- As pegadas digitais, com base na possibilidade ou não de serem influenciadas por um utilizador, podem geralmente ser divididas em pegadas que podem ser influenciadas (activas) e as que não podem (passivas).
- No mundo das TIC, aplica-se uma regra: sempre que carrega, transfere, medeia ou coloca algo no ciberespaço, ele fica lá "para sempre". As pegadas passivas surgem mais frequentemente da interacção de um sistema informático com outro sistema informático ou da funcionalidade de um sistema informático (e software associado). Exemplos de tais pegadas podem ser informações do sistema operativo (tais como mensagens de erro do Windows ou informações do sistema), ou outras informações e dados que são armazenados com base na funcionalidade do sistema sem terem de ser transmitidos (tais como um sistema informático que nunca foi ligado a qualquer rede ou outro sistema informático). Dizer de forma totalmente intransigente que estas pegadas não podem ser influenciadas não seria inteiramente correcto. Se um utilizador tiver experiência suficiente, é capaz de alterar, mascarar ou suprimir uma série de pegadas digitais "passivas" (por exemplo, através de um simples modo anónimo do navegador da web que desliga os cookies). No entanto, o movimento de um utilizador na Internet pode ser monitorizado de várias maneiras.
- Uma pegada digital activa que pode ser influenciada representa toda a informação que um utilizador transfere voluntariamente sobre si próprio para outra pessoa (quer seja natural ou legal, ou mesmo ISP). A transferência pode incluir uma série de actividades, tais como o envio de um correio electrónico, adição de um post a uma discussão, fórum, publicação de qualquer meio de comunicação (foto, vídeo, áudio, etc.) em meios de comunicação social, etc. O termo também inclui um registo e utilização de todos os serviços concebíveis no ciberespaço [por exemplo, sistemas operacionais, e-mails (incluindo freemail), redes sociais, encontros, redes P2P, chats, blogs, quadros de avisos, websites, serviços de nuvem, armazenamento de dados, etc.].

PALAVRAS-CHAVE A LEMBRAR

- Pegada digital
- Pegada digital passiva
- Pegada digital activa
- EULA

PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- Definir o termo "pegada digital".
- Como é que as pegadas digitais diferem umas das outras?
- Em que elementos consiste uma pegada digital passiva?
- Quem é o LIR?
- Que informação sobre um utilizador transporta um endereço IP?
- O que é o EULA?

Conclusão

Com a utilização de tecnologias de informação e comunicação e o volume sempre crescente de dados publicados pelos utilizadores, houve necessariamente pedidos de supressão ou apagamento de dados que estão desactualizados ou que de alguma forma prejudicam um utilizador.

A visão de que o mundo digital e os seus utilizadores se tornarão anónimos é, a meu ver, uma utopia. As várias possibilidades de anonimização sob a forma, por exemplo, de serviços de rede TOR[204] , etc., não mudarão nada nesta afirmação, pois haverá sempre interacções com o mundo real. Além disso, haverá sempre utilizadores no mundo digital que são falíveis e que cometem erros, por muito bem que tentem esconder informações sobre as suas actividades. É também uma utopia pensar que a tecnologia irá esquecer. Continuarão a ser recolhidos dados sobre os utilizadores. O que irá acontecer será outro cenário técnico de quem irá ver os dados e de quem não irá.

Sem dúvida, a interligação dos serviços individuais oferecidos e a possibilidade de passar informações sobre os utilizadores a terceiros, bem como a **Internet das Coisas (IoT)**, contribuem para a "desanonimização" dos utilizadores.

Por exemplo, o Facebook apresentou uma solução interessante para a "desanonimização" dos utilizadores, desenvolvendo o método **DeepFace**, que se baseia na criação de um modelo 3D do rosto com base em pontos de partida definidos numa fotografia.[205] Com base neste método, é também possível identificar pessoas que não têm uma conta no Facebook e que apenas foram marcadas (identificadas) como uma pessoa específica. O método DeepFace é aqui intencionalmente mencionado, uma vez que a possibilidade de utilizar este método está consagrada nos Termos de Serviço do Facebook e permite, mesmo que um utilizador não o deseje fazer (por exemplo, não se marque intencionalmente sob uma fotografia), a sua identificação.

Quanto à **IOT**, a intervenção das novas tecnologias e a nossa "desanonimização" é ainda mais aparente. Como exemplo, mencionarei uma "smart TV"[206] , que durante a instalação efectiva oferecerá novamente os Termos de Serviço para aprovação e imediatamente a seguir "perguntar" sobre a possibilidade de ligação à Internet. Por exemplo, uma análise mais detalhada dos Termos de Serviço pode indicar que esta televisão está autorizada a fornecer um registo de chamadas ou actividades confidenciais e presenciais que "*realiza*", desde que utilize o controlo de voz ou movimento. Como parte dos Termos de Serviço, será também notificado de que os dados gravados são transmitidos ao fabricante e a terceiros. A única solução para evitar que esta informação seja transmitida é desligar o reconhecimento de voz ou de movimento. A questão é saber se esta é realmente a solução. Pessoalmente, penso que a solução seria desligar ou restringir a transferência de dados, ou identificar a entidade com a qual estou disposto a partilhar estes dados pessoais.

Quanto ao direito a ser esquecido, posso imaginar uma situação hipotética em que um utilizador irá solicitar que a empresa que produziu a televisão ou outro sistema informático com Termos de Serviço semelhantes apague o registo de chamadas, por exemplo, a partir de 1 de Março de 2016. O tribunal

[204] Alguns casos de violações de segurança de redes TOR:
O FBI Explora a Vulnerabilidade Flash para Violar a Segurança da Rede Tor. [online]. [cit.23/07/2016]. Disponível em: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/
Aconselhamento de segurança Tor: "retransmissão antecipada" de ataque de confirmação de tráfego. [online]. [cit.23/07/2016]. Disponível a partir de:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

[205] Para mais detalhes, ver, por exemplo *O Facebook poderá em breve identificá-lo em qualquer fotografia.* [online]. [cit.09/08/2015]. Disponível a partir de: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

[206] Ver também, por exemplo, ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit.09/08/2015]. Disponível em: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

aplica o direito de "ser esquecido" também neste caso, mas a questão é quem irá realmente garantir ao utilizador que os seus dados foram apagados de todos os repositórios de dados.

Excerto do EULA da Samsung:

Tenha em atenção que, se as suas palavras faladas incluírem informações pessoais ou outras informações sensíveis, essas informações estarão entre os dados capturados e transmitidos a terceiros através da sua utilização do Reconhecimento de Voz.

Não existe anonimato na Internet e certamente não existirá num futuro próximo. Os utilizadores lutam frequentemente, de forma bastante lógica e justificada, contra a intervenção do Estado na sua privacidade, mas por outro lado, eles próprios oferecem esta informação privada voluntariamente e com muito mais vontade a todos os que os rodeiam (por exemplo, nas redes sociais, nos serviços de nuvem, etc.).

Não penso que o fosso entre o mundo real e o mundo digital seja tão grande. Talvez seja por isso que muitas vezes não compreendo o comportamento irreflectido dos utilizadores quando se trata dos serviços oferecidos pelos ISPs. Sim, como utilizadores, receberemos um serviço ao abrigo dos Termos de Serviço em que entramos. A questão é saber se este acordo é vantajoso e se o preço que pagamos por este serviço é razoável.

Pessoalmente, estou plenamente consciente de que a minha liberdade, incluindo um grau de "anonimato" na Internet, já é uma utopia. Acredito que num futuro próximo, graças à IOT e à interligação cada vez maior de todos os "serviços", esta utopia será quase colocada numa situação, não muito diferente da que consta do *Relatório Minoritário.* Por outro lado, acredito, ou melhor, quero acreditar, que ainda estou livre e tenho o direito de escolher.

Este direito à minha escolha reside então pelo menos na minha decisão se, ou que serviços quero utilizar e sob que condições. Penso que os utilizadores devem tornar-se a verdadeira autoridade definidora da Internet, pelo menos na forma em que mostram a sua vontade e tentam ganhar os seus direitos para o fornecedor de serviços porque, no caso de intervenção do Estado na sua privacidade, em muitos casos são bem sucedidos.

Afinal, para avaliar quão "agressivo" é o serviço, ou o quanto interfere com a sua privacidade, pode ser encontrado, por exemplo, no website: Termos de Serviço, Não Lido: https://tosdr.org/. Se nada mais (embora seja possível utilizar a analogia de "Digital Dementia"), então pelo menos a verificação dos termos básicos nesta página pode ajudar os utilizadores a estarem mais bem informados sobre o assunto.

Vivemos numa época em que as tecnologias de informação e comunicação já estão indissociavelmente ligadas a todos os aspectos do nosso ser. Um certo paradoxo é que essencialmente não temos a oportunidade de evitar esta penetração e interacção mútua com as TIC, o que, ao mesmo tempo, nos torna mais vulneráveis.

Devido às tecnologias de informação e comunicação e aos serviços interligados, criamos um reflexo da nossa identidade ou personalidade no mundo virtual.

O nosso "eu" digital tem todos os pré-requisitos para ser "muito mais durável" do que o nosso corpo físico. As informações sobre as nossas actividades no ciberespaço, as nossas personalidades cibernéticas, os nossos relatos e as nossas pegadas digitais viverão após a nossa morte, graças ao arquivamento de dados e informações sobre nós.

medida que o volume de dados e informações armazenadas em cada FSI cresce, as questões da sua segurança efectiva, transferência ou eliminação são cada vez mais abordadas, não só com base num contrato celebrado entre o prestador de serviços e o utilizador final, mas também com base em legislação emergente.

Estados, organizações e indivíduos estão cada vez mais conscientes de que a informação e os dados representam um potencial significativo, que é cada vez mais atacado por ciberataques, quer com o objectivo de roubo, dano, inacessibilidade ou eliminação de dados.

Se quisermos viver na sociedade actual e tirar partido dos seus benefícios, não é possível livrarmo-nos das TIC, e definitivamente não faz sentido deixar de utilizar estas tecnologias. É necessário começar a aprender como utilizar estas tecnologias e serviços e como evitar, ou pelo menos eliminar, as consequências dos ciberataques.

No ciberespaço, como no mundo real, não existe um único tipo de segurança ou protecção que possa ser aplicado universalmente a todos. Se queremos abordar a segurança, precisamos de a abordar de forma abrangente, e precisamos de a adaptar a cada indivíduo.

Lista de fontes utilizadas

1. ANGWIN, Julia. *Conheça o Dispositivo de Rastreio Online que é Virtualmente Impossível de bloquear.* [online]. [cit.10/06/2016].
2. BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit.23/09/2014]. Disponível em: https://www.eff.org/cyberspace-independence.
3. CAETANO, Lianne. *As suas aplicações estão a ser sobre-partilhadas? O Relatório de Segurança Móvel de 2014 diz tudo.* [online]. [cit.10/04/2015]. Disponível a partir de: https://blogs.mcafee.com/consumer/mobile-security-report-2014/
4. ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit.09/08/2015]. Disponível em: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx
5. *CNN sobre sexo pedófilo no Second Life.* [online]. [cit.18/06/2009]. Disponível em: http://www.youtube.com/watch?v=AQM-SiiaipE
6. *População mundial actual.* [em linha]. [cit.10/08/2015]. Disponível em: http://www.worldometers.info/world-population/
7. Ver também: *Estatísticas interessantes sobre Estratégias Móveis para Transformações Digitais.* [online]. [cit.15/07/2016]. Disponível em: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/
8. *Retenção de dados inconstitucional na sua forma actual.* [em linha]. [cit.16/07/2016]. Disponível a partir de: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690
9. *Delokalizace právních vztahů na internetu* [online]. [cit.15/04/2012]. Disponível em: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html
10. *Digital, Social & Mobile Worldwide em 2015.* [online]. [cit.09/08/2015]. Disponível a partir de: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/
11. ENGLEHARDT, Steven e Ardvin NARAYANANAN. *Seguimento em linha: Uma medição e análise de 1 milhão de sítios.* [em linha]. [cit.05/08/2016]. Disponível a partir de: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf
12. *O Facebook poderá em breve identificá-lo em qualquer fotografia.* [online]. [cit.09/08/2015]. Disponível a partir de: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo
13. *O FBI Explora a Vulnerabilidade Flash para Violar a Segurança da Rede Tor.* [online]. [cit.23/07/2016]. Disponível em: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/
14. *Primeira Emenda.* [em linha]. [cit.10/07/2016]. Disponível a partir de: https://www.law.cornell.edu/constitution/first_amendment
15. *O Bundestag alemão aprova a nova lei de retenção de dados.* [em linha]. [cit.16/07/2016]. Disponível em: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/
16. GREENFIELD, David. *Integrovaná bezpečnost: Uz nastal její čas?* [online]. [cit. 01/03/2018]. Disponível a partir de: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/.
17. HAINES, Lester. *Jogador online apunhalado por palavras cibernéticas "roubadas".* [online]. [cit.03/10/2006]. Disponível em: http://www.theregister.co.uk/2005/03/30/online_gaming_death/
18. http://news.bbc.co.uk/2/hi/technology/6638331.stm
19. http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html
20. HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praga: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, pp. 101-102.
21. *Censura da Internet.* [em linha]. [cit.10/08/2016]. Disponível em: http://www.deliveringdata.com/2010_10_01_archive.html
22. *História da Internet na década de 1980.* [em linha]. [cit. 07/06/2016]. Disponível em: http://www.computerhistory.org/internethistory/1980s/
23. *Internet, připojení k němu a možný rozvoj (Část 2 - Historie a vývoj Internetu).* [online]. [cit.10/02/2008]. Disponível a partir de: http://www.internetprovsechny.cz/clanek.php?cid=163
24. JOHNSON, David R. e David POST. *A Ascensão da Lei no Ciberespaço.* [online]. [cit.10/07/2016]. Available from: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067043023001058093120070084069085089012000019127120091078115090125017120030014000101095031109003094069069113114112102&EXT=pdf

25. KODET, Jaroslav. *Kybernetický zákon: Vyuuzijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Disponível em: https:**//www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf**
26. KOLOUCH, Jan e Andrea KROPÁČOVÁ. Responsabilidade pelo Dispositivo Próprio e Dados e Aplicações nele Armazenados. In: *Avanços na Ciência da Informação e Aplicações Volume I: Actas da 18ª Conferência Internacional sobre Computadores (parte do CSCC '14).* [B.m.], c2014, pp. 321-324. Série Avanços Recentes em Engenharia Informática, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.
27. KOLOUCH, Jan e Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praga: Academia de Polícia da República Checa em Praga, 2013, p. 65
28. KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 78 e seguintes e p. 109 e seguintes.
29. KOLOUCH, Jan. Pseudoanonymita - bezpečnostní riziko pro uzivatele Internetu. *DSM - gestão de segurança de dados* [online]. 2015. Vol. 19, No. 3, pp. 24-29 ISSN 1211-8737. Disponível em: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/
30. *Redes sociais líderes a nível mundial a partir de Abril de 2016, classificadas por número de utilizadores activos (em milhões)* [online]. [cit.10/08/2015]. Disponível em: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
31. LESSIG, Lawrence. *Código v. 2. p.* 6 Disponível na íntegra (Eng) [online]. [cit.13/03/2008]. Disponível a partir de: http://pdf.codev2.cc/Lessig-Codev2.pdf
32. MAISNER, Martin e Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praga: Wolters Kluwer, 2015. p. 85
33. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praga: CZ.NIC, 2013. ISBN 978-80-904248-7-6 p. 25
34. *Desafios jurídicos nacionais à Directiva de Retenção de Dados.* [em linha]. [cit.16/07/2016]. Disponível em: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
35. *Největší sociální sítě na světě? Facebook je sice jednička, ale...* [online]. [cit.10/08/2015]. Disponível em: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/
36. *Ciclo PDCA.* [online]. [cit. 06/07/2018]. Disponível em: https://www.creativesafetysupply.com/glossary/pdca-cycle/
37. PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám uz uz EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10/11/2015]. Disponível em: http://www.earchiv.cz/b14/b0428001.php3
38. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 7
39. PO`ÁR, Josef e Luděk NOVÁK. *Pracovní příručka bezpečnostního manaizera.* Praga: AFCEA, 2011. ISBN 978-80-7251-364-2, p. 5, ou: PO`ÁR, Josef e Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Disponível em: https://www.cybersecurity.cz/data/srib.pdf p. 1
40. REED, Chris. *Direito da Internet*. Cambridge: Imprensa da Universidade de Cambridge, 2004, p. 218
41. *Registos regionais da Internet.* [em linha]. [cit.04/08/2015]. Disponível em: https:*//www.nro.net/about-the-nro/regional-internet-registries*
42. ROSER, Christoph. *The Many Flavors of the PDCA.* [em linha]. [cit. 06/07/2018]. Disponível em: https://www.allaboutlean.com/pdca-variants/
43. ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10/11/2017]. Disponível a partir de: https:*//www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*
44. SMEJKAL, Vladimír. *Internet a §§§.* 2ª actualização. e ext. ed. Praga: Grada, 2001, p. 32
45. SMITH, Craig. *Pelos Números: 100 Fatos e Estatísticas de Pesquisa Incríveis do Google.* [online]. [cit. 04/08/2016]. Disponível em: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/
46. O Tribunal de Justiça da União Europeia. Comunicado de imprensa n.º 54/14, datado de 8 de Abril de 2014. Acórdão nos processos apensos C-293/12 e C-594/12. [em linha]. [citado 15/07/2016]. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf
47. SPITZER, Manfred. *Digitátlní demence.* Brno: Hospedeiro, 2014. ISBN 978-80-7294-872-7
48. Conclusões do Advogado-Geral Pedro Cruz Villalón. Processo C-293/12 e C-594/12. [em linha]. [cit.15/07/2016]. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954
49. Conclusões do Advogado-Geral SAUGMANDSGAARD ØE, de 19/07/2016. Nos processos apensos C-203/15 e C-698/15. [em linha]. [citado 10/8/2016]. Disponível a partir de: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650
50. ŠTOČEK, Milão. V *Hitlerově duchu proti Hitlerovi.* [online]. [cit.10/07/2016]. Disponível em: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325
51. *Surface Web, Deep Web, Dark Web - What's the Difference.* [em linha]. [cit. 20/07/2016]. Disponível em: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

52. *A teia escura explicada.* [em linha]. [cit. 20/07/2016]. Disponível em: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
53. *A fragmentação do Android tem novos registos: 24 000 dispositivos diferentes.* [em linha]. [cit.15/07/2016]. Disponível a partir de: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/
54. *O primeiro malware móvel: como Kaspersky Lab descobriu Cabir.* [online]. [cit.01/08/2016]. Disponível a partir de: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
55. THOMAS, Douglas. *A criminalidade na Fronteira Electrónica.* Em Cibercriminalidade. Em Londres: Routledge, 2003, p. 17 e seguintes.
56. *Aconselhamento de segurança Tor: "retransmissão antecipada" de ataque de confirmação de tráfego.* [online]. [cit.23/07/2016]. Disponível a partir de:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack
57. TRADOC. Operações de Ciberespaço: Plano de Capacidade do Conceito 2016-2028. [em linha]. [cit. 18/02/2018], pp. 8-9 Disponível em: www.fas.org/irp/doddir/army/pam525-7-8.pdf?
58. VO'ENÍLEK, David. *Promazání "sušenek" nepomůže, na internetu vás prozradí i baterie.* [online]. [cit.04/08/2016]. Disponível a partir de: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz
59. *World Internet Users and 2015 Population Stats.* [em linha]. [cit.09/08/2015]. Disponível em: http://www.internetworldstats.com/stats.htm
60. *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají moňost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit.04/04/2014]. Disponível a partir de: https://www.google.cz/intl/cs/policies/?fg=1