# O DIREITO CIBERNÉTICO E AS TÉCNICAS DE CRIPTOGRAFIA

**PINTO FERREIRA**

A palavra criptografia provém do grego, cabendo relembrar que o Direito Cibernético usa várias palavras com esta origem, como criptografia e cibernética. Esclarecendo tal significado escreve um vernaculista de renome Aurélio Buarque de Holanda, expondo o seguinte pensamento: "criptografia. (De cript(o) - + grafia). S.f. 1. Arte de escrever em cifra ou em código. 2. Conjunto de técnicas que permitem criptografar informações (como mensagens escritas, dados armazenados ou transmitidos por computador etc.)".

Vejamos algumas definições dadas sobre criptografia. Escreve Wilson José de Oliveira, em seu livro *Hacker. Invasão e proteção* (Florianópolis, Ed. Visual Books, 1999, p. 339), sobre a origem e o conceito desta palavra:

"Vem do grego, kriptos=escondido oculto + grafia, é a arte ou ciência de escrever em cifra ou em códigos, seria então um conjunto de técnicas que tornam uma mensagem incompreensível, permitindo apenas que o destinatário, que conhece a chave de encriptação, consiga desencriptar e ler a mensagem com clareza. Existem pessoas que, por meios ilícitos, podem ter acesso à mensagem cifrada e determinar a chave de encriptação. Estes se chamam de criptoanalistas, que não fazem nada mais que a decomposição da mensagem sem conhecer a chave, quebrando o sistema."

A criptografia é por conseguinte uma arte, a arte de escrever ocultamente. Pretende-se que ela é tão antiga quanto a própria escrita e atualmente é na verdade um dos meios mais eficazes da transmissão e da transferência de informações e dados, sem que exista possibilidade de comprometimento do sigilo e do segredo.

A criptografia é assim uma maneira expressiva e segura da guarda de mensagens e da transmissão de dados, sobretudo hoje em dia em que se procura segurança por causa dos crimes cibernéticos.

Há duas formas concretas de criptografia: a criptografia tradicional e a criptografia eletrônica, com o surgimento dos computadores eletrônicos. Este último sendo o núcleo dessa derradeira espécie.

Já Júlio Cesar enviava informações para os seus comandos políticos e militares através de mensagens cifradas, usando letras do alfabeto, por exemplo, substituindo uma letra a ou b por uma outra. Trata-se de uma criptografia manual, hoje em dia praticamente em desuso, visto que surgiu a era da informática e da eletrônica consagrando uma segunda revolução industrial, que se seguiu à primeira, com as chamadas civilizações das chaminés, do carvão e da máquina a vapor.

A transmissão de dados é feita a longa distância e florescendo sobre a informática apareceu a telemática. A telemática é a transmissão de dados ou de informações entre computadores eletrônicos distantes uns dos outros, ou de longitudes diferentes, comunicação essa feita mediante linhas telefônicas, fibras óticas, microondas e cabos coaxiais. O nome deriva da conjunção de *tele + informática* ou *tele + eletrônica*. Todo esse sistema recebe hoje o nome de telemática.

A criptografia tem hoje uma importância extraordinária, é um grande meio de defesa e de segurança pública do Estado. Nos Estados Unidos por exemplo a criptografia está relacionada com a própria defesa do Estado norte-americano, é incluída inclusive como arma ou instrumento de defesa para proteção legal. De conformidade com "Arms Export Control Act" ou Lei de Controle à Exportação de Armas, é um artigo de defesa do país, como uma arma, para a segurança nacional, com medidas proibitivas de exportação de softwares criptográficos

Houve até discussões judiciais sobre esta proibição resolvidas pela Suprema Corte Americana, que permitiu a exportação tão-somente de chaves de no máximo 40 bits, isto por causa do tamanho medíocre da chave criptográfica.

Em 1° de outubro de 1996, o Vice-Presidente Al Gore permitiu e autorizou a exportação de softwares criptográficos, por dois anos, isto é, com programas que utilizassem uma chave de até 56 bits e depois do decurso desses dois anos somente com chaves de até 40 bits.

Atualmente o sistema de criptografia do governo tem até 100 quintilhões de chaves.

O que se deve entender pela palavra chave em criptografia? A chave pode ser uma palavra, como também uma frase ou uma seqüência aleatória de números. A dimensão ou o tamanho da chave é mensurado em bits, quanto maior for a chave mais seguro se torna o sistema criptográfico. Esta chave pode ser pública ou privada.

Vejamos algumas definições de criptografia de alguns autores que se especializaram na matéria. De acordo com Gustavo Testa Correia em seu livro *Aspectos jurídicos da internet* (São Paulo, Ed. Saraiva, 2000, p. 77):

"A criptografia seria uma 'máscara' colocada sob determinado arquivo, tornando-o irreconhecível para aqueles que lhe 'olhassem na rua', ou seja, algo lógico, relacionado a fórmulas matemáticas, e só alguém que possuísse a fórmula matemática certa poderia desmascará-la e, assim, lê-la."

Segundo o Prof. Daniel Bernestein, a criptografia "é a arte e a ciência de manter mensagens, que serão compartilhadas, seguras".

Neil Barret em seu livro *Digital Crime* (Londres, Kogan Page, 1997) considera que a criptografia pode ser entendida como "a aplicação de séries complexas de algoritmos sob determinados dados".

A criptografia tradicional tem origem remota, porém a criptografia moderna e eletrônica já resulta de trabalhos e experimentos feitos pela IBM por volta de 1960, com mudanças com a velocidade vertiginosa acompanhando o progresso nos computadores, já em sua quinta geração.

É importante também mencionar alguns conceitos básicos ligados à matéria, a saber, encriptar, encriptação, desencriptar, desencriptação, chave, enquanto outros são utilizados em vários outros ramos do conhecimentos, como bit e bytes, com os seus significados já conhecidos.

A palavra encriptar procede da língua inglesa *encrypt*, como os seus derivados e termos assemelhados, com o significado em informática que é o seguinte: codificar os sinais de um programa ou de uma transmissão para que seja evitada a sua utilização indevida. Encriptação é um substantivo. No mesmo sentido escreve Wilson José de Oliveira (cit., p. 340): "Em um sistema criptográfico típico utilizam-se as operações de ciframento e deciframento. O que ocorre na operação de deciframento é normalmente o inverso do ciframento."

O nome "*bit*" significa a unidade mínima de informação em um sistema digital, podendo assumir somente um de dois valores, geralmente 0 ou 1. É assim uma programação bivalente ou um sistema binário. Etnologicamente resulta do inglês da combinação das iniciais de *(bi)nary* e *digi(t)*.

Tem-se agora a expressão "*byte*", que também procede etnologicamente do inglês "*binary*" e "*term*", com o sentido de termo binário, entendida como seqüência constituída por um número fixo de bits adjacentes, e cuja dimensão ou comprimento é de 8 bits.

Já a expressão algoritmo usada na criptografia emana do latim medieval "*algorithmos*", que por sua vez tem a sua origem grega de "arithmós" ou número, de onde também vem a palavra universalmente conhecida de aritmé-

tica. O algoritmo na informática é o conjunto de regras e operações bem caracterizadas e ordenadas, com a finalidade de resolver um problema, uma classe de problemas, em um número finito de etapas.

Resta emoldurar esta exposição com o conceito de chave na informática. Chave, palavra que deriva do latim clave, com uma versão popular, assim significando na informática: é uma senha para o acesso ou a entrada de um sistema, programa ou dado de conteúdo limitado e restrito.

Os Hackers podem utilizar muitos tipos de ataques ao texto cifrado e daí a necessidade de um sistema de defesa que é o sistema criptográfico, com sua metodologia própria para impedir o ataque dos invasores.

Existem assim diferentes métodos de defesa distinguindo-se sobretudo os métodos da criptografia tradicional e os métodos da criptografia computacional. E ainda a utilização de métodos mediante chave privada e chave pública.

Apreciando os métodos de criptografia tradicional cabe relembrar a existência de 3 metodologias, a primeira usando cifras de substituição, a segunda mediante o emprego de cifras de transposição e a terceira mediante códigos e máquinas de cifragens.

Atualmente esta metodologia está sendo acompanhada da outra mais moderna que é a criptografia computacional de chave única, na qual todas as operações são implementadas mediante um computador ou ainda por um circuito especial.

O modelo mais conhecido de cifrador computacional de chave única é o DES ("Data Encyption Standard"), que foi feito e desenvolvido pela IBM e aceito logo como padrão nos Estados Unidos em 1997, o DES faz a cifragem com blocos de 64 bits, correspondendo a 8 caracteres, mediante o uso de uma chave de 56 bits, acrescidos de 8 bits de paridade, totalizando 64 bits.

A respeito escreve Wilson José de Oliveira (cit., p. 343): "O que ocorre é que o algoritmo inicia uma transposição sobre os 64 bits da mensagem, seguida de 16 passos de cifragem e conclui realizando uma transposição final que é inversa a da transposição inicial. As transposições são independentes da chave. Portanto, serão utilizados 16 passos de cifragem com as 16 subchaves, todas criadas a partir da chave original através de deslocamento e transposições. Cada passo vai dividir o bloco em duas metades de 32 bits (L e R) e realizar transposições, substituições, expansões (duplicações) de bits e redução (eliminação) de bits, além de utilizar operações lógicas do tipo ou exclusivo. O DES exerce uma cifragem com dois objetivos: difusão e confusão. Difunde eliminando a redundância da mensagem original e confunde tornando a chave tão complexa quanto possível, mudando as características da mensagem original."

Quando apareceu o DES foi objeto de muitas críticas, porém com modificações surgiram outros modelos firmados pelo padrão original.

Além do aperfeiçoamento do DES planejado pela IBM, surgiram inúmeros outros métodos, tais como: o modo do Livro de Código (Electronic Code Book — ECB), o modo de Encadeamento de Blocos (Cipher Block Chaining — CBC); o modo de Realimentação de Cifra (Cipher Feedback — CFB); o modo de Encadeamento de Blocos (Block Chaining); o modo de Encadeamento Propagado (Propagating Cipher Block Chaining — PCBC).

Não se pode também deixar de apreciar o problema das chaves privadas e das chaves públicas utilizadas no sistema criptográfico.

A encriptação com chave privada é o método de encriptação fazendo uso de uma mesma chave tanto para encriptar como para desencriptar a mensagem transmitida. Esta chave pode ser tanto uma frase, ou também uma seqüência aleatória de números, sendo o número de chaves medidos em bits e também através de números. O sistema é tanto mais seguro quanto maior for o tamanho da frase ou da numeração prevista.

A encriptação por chave pública é de certo modo mais aperfeiçoada e oferece maior segurança. O receptor da mensagem tem as suas próprias chaves que ele cria e imagina e que são inter-relacionadas, e que só a ele pertencem, sendo uma chave pública e outra privada. A chave pública é de distribuição livre. O transmitente da mensagem só pode utilizar a chave pública para o processo de encriptação ou de codificação. A mensagem codificada ou encriptada somente pode ser conhecida, desencriptada ou decodificada pelo receptor, que possui a detenção da chave privada.

Afinal, no tocante à legislação, cabe salientar que no Brasil existe o Decreto n. 2910, de 29 de dezembro de 1998, estabelecendo regras para a salvaguarda de documentos, materiais, áreas, comunicações de dados de natureza sigilosa, sem referência ao tamanho máximo das chaves.

A criptografia é uma arma de defesa para a segurança do Estado e do cidadão. Porém pode ser utilizada para fins criminais. Daí a necessidade de leis específicas contra os crimes cibernéticos, sobre as quais já existem vários projetos de lei transitando no Congresso Nacional, entre os quais o do Deputado Federal de Pernambuco, Luiz Piauhylino (Projeto de Lei n. 84, de 1999), do ex-ministro Renan Calheiros, e do Deputado estadual pela Paraíba Cassio Cunha Lima (Projeto de Lei n. 1713, de 1996) e da Resolução CGIB n. 1, de 15 de abril de 1998.

Em suma, o sistema criptográfico é uma poderosa muralha de defesa das mensagens e das comunicações de dados.