



Projeto Mário Travassos

Artigo de Opinião

A difusão da lei 12.737/2012 no âmbito do Exército Brasileiro

Cap Atilla Rodrigo Pereira Silva

(Opinião de inteira responsabilidade do autor)

2022

Resumo

Este estudo discorre sobre a possibilidade de aplicação da Lei nº 12.737/2012 nas unidades do Exército Brasileiro. Buscou-se verificar as possibilidades de difusão das normatizações nos aquartelamentos do Exército. Foi realizada uma pesquisa bibliográfica sobre a Lei nº 12.737/2012 e sua importância para o direito digital do país, conjuntamente com uma análise da relevância da lei no âmbito castrense e suas possíveis aplicações.

Palavras-Chaves: Lei nº 12.737/2012. Exército Brasileiro.

Introdução

O desenvolvimento digital acarretou transformações no cotidiano de nossa sociedade. Crescentemente, as pessoas utilizam os meios digitais para realizar suas atividades rotineiras, sendo a internet o principal meio integrador de tais ações.

No entanto, com as benesses geradas pela evolução cibernética, surgiram diversas práticas ilícitas que se utilizam desse instrumento digital, os denominados crimes cibernéticos. (COSTA, 2022).

Dentre os ilícitos, podemos citar o ataque hacker ocorrido no ano de 2021, no site do Ministério da Saúde, em que os portais “ConecteSUS” e o “Portal Covid”, ferramentas utilizadas na gestão do combate à pandemia do COVID-19, ficaram indisponíveis por 15 dias após o ataque do grupo Lapsus\$ (ANDRADE, 2021).

Mediante esse escopo, é importante destacar a evolução jurídica alcançada sobre o assunto no país durante os últimos dez anos, como a sanção da lei nº 12.737/12, que trata sobre a tipificação criminal dos delitos ocorridos pela internet em território nacional.

Não obstante, acompanhando a revolução cibernética, o Exército Brasileiro está digitalizando seus processos operacionais e administrativos, a fim de alcançar a eficiência de suas ações e abreviar o tempo gasto em suas atividades.

Concomitantemente, é significativo asseverar que, como órgão público, a lei 12.737/12 aplica-se aos militares que utilizam meios digitais nos aquartelamentos castrenses, fato considerável para que exista uma possível exploração do conteúdo por meios de instruções nas escolas de formação e quartéis do Exército Brasileiro.

Desenvolvimento

A elaboração da Lei Nº 12.737 de 2012 ocorreu após o Congresso Nacional verificar que o nosso país vivenciava uma lacuna jurídica em relação aos crimes cometidos de forma digital.

Nos anos anteriores, existia uma inerente dificuldade em tipificar os delitos ocorridos pela internet, pois, com a utilização desse novo tipo de comunicação, era observado o conflito de alguns direitos já sancionados, como por exemplo, a proteção à honra. (SANTANA, 2021).

Durante os diversos estudos e discussões que estavam ocorrendo sobre o tema, houve, em maio de 2012, a invasão do computador da atriz Carolina Dieckmann, sendo trinta e seis fotos pessoais expostas na rede digital sem a sua permissão.

Os crackers, usuários da internet que pirateiam programas (LIMA, 2021), inseriram um determinado vírus de computador numa máquina de processamento de dados da artista e pediram dez mil reais a fim de não expor seus arquivos. Como não foram atendidos, minutos depois, seus arquivos estavam sendo acessados por milhares de pessoas (SANTANA, 2021).

Diante disso, foi aprovado o projeto de lei número trinta e cinco, elaborado pelo deputado federal Paulo Teixeira o qual, em 30 de novembro de 2012 foi sancionado e converteu-se na lei 12.737 de 2012, conhecida como lei Carolina Dieckmann (BEZERRA, 2021).

Analisando a legislação jurídica, observa-se que vários delitos tipificados como crime podem ser praticados por militares com acesso à Internet, inclusive utilizando o computador de uma organização militar.

Exemplificando tal fato, pode-se afirmar que o Exército é uma instituição que possui dados sigilosos e a publicação indevida desses assuntos podem ser qualificados como delitos:

§3 Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (BRASIL,2012).

De forma a elucidar o tema, podemos citar, também, a preocupação do Exército Brasileiro com o assunto, destacando, assim, as Instruções Gerais de Segurança da Informação para o Exército Brasileiro - (IG 20-19), onde orienta aos militares castrenses em trabalharem com mínima exposição, devendo utilizar ações de

contingência, com a finalidade de mitigar os riscos atinentes à utilização da rede mundial de computadores nos estabelecimentos do Exército Brasileiro.

Além disso, o documento elenca objetivos a serem cumpridos nas unidades militares, sendo que, um dos sete, é desenvolver o esclarecimento dos militares em relação ao uso seguro dos meios cibernéticos:

III - fomentar, ao longo de toda a cadeia hierárquica, a obtenção de atitude favorável no tocante à Segurança da Informação, bem como incrementar a conscientização a respeito da importância do assunto; IV - estimular a eliminação da dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação e de comunicações; V - promover o intercâmbio científico tecnológico, junto a outros órgãos da Administração Pública Federal e instituições públicas e privadas, sobre as atividades de Segurança da Informação; VI - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em Segurança da Informação; e VII - promover a interoperabilidade e a integração dos sistemas de informação, não só no âmbito do Exército mas, também, junto às demais Forças Armadas e aos demais órgãos da Administração Pública Federal, quando julgado pertinente e respeitadas as regras e normas de segurança em vigor (IG 20-29 INSTRUÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO PARA O EXÉRCITO BRASILEIRO, 2001, p.8).

Conclusão

Após o estudo do tema, verifica-se a importância da divulgação da Lei 12.737 de 2012 nas unidades do Exército Brasileiro. É notório salientar que tal medida objetiva atenuar possíveis delitos que possam ser cometidos em estabelecimentos castrenses, muitas das vezes, por desconhecimento do ordenamento jurídico atual.

Cita-se, também, que tal evento, propicia desenvolvimento da consciência situacional sobre a segurança cibernética, ato que deverá estar presente na cultura organizacional da instituição, tendo em vista o aumento da digitalização dos métodos e procedimentos.

Por fim, pode-se afirmar que a metodologia de divulgação poderá ocorrer através de instruções específicas durante o ano de instrução para oficiais e praças ou com a inclusão do tema no currículo das escolas de formação, sendo estes possíveis propagadores do presente conhecimento aos futuros integrantes da força terrestre brasileira.

Referências

ANDRADE Henrique. **Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar**. Disponível em: <<https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-taquehacker-durante-madrugada-e-sai-do-ar/>>. Acesso em: 31 ago.2022. [://riec.univs.edu.br/index.php/riec/article/view/246/195](http://riec.univs.edu.br/index.php/riec/article/view/246/195).

BRASIL. Exército. PORTARIA Nº 483, DE 20 DE SETEMBRO DE 2001. IG 20-19 - Instruções Gerais de Segurança da Informação para o Exército Brasileiro. **Boletim do Exército**, Brasília, DF, 2001.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2848 de 7 de dezembro de 1940 – Código Penal; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 3 dez. 2012.

BEZERRA, João Manoel de Vasconcelos. **Aplicabilidade da lei nº 12.737/12 sobre crimes cibernéticos**. Disponível em: <<https://riec.univs.edu.br/index.php/riec/article/view/246/195/>> Acesso em: 31 ago. 2022.

COSTA, Igor Duarte Suguimoto. **Cibercriminalidade: origem e evolução dos crimes cibernéticos**. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3794/>> Acesso em: 31 ago. 2022.

LIMA, Cláudio Vieira Guimarães. **Crimes cibernéticos: o lado obscuro da rede**. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2419/>> Acesso em: 31 ago. 2022.

SANTANA, Gabriel Còvolo. **Crimes cibernéticos: necessidade do aprimoramento da tipificação penal dos crimes cibernéticos**. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3089/>> Acesso em: 31 ago. 2022.

SANTANA, Roque Felipe da Silva. **Crimes cibernéticos: análise evolutiva da legislação penal brasileira e seus desafios**. Disponível em: <<https://ri.ucs.br:8080/jspui/bitstream/prefix/4456/1/TCCROQUESANTANA/>> Acesso em: 31 ago. 2022.