

RECOMENDAÇÕES GERAIS AOS POLICIAIS MILITARES DO DF PARA O USO DA INTERNET E REDES SOCIAIS

I – FINALIDADE

A Polícia Militar do Distrito Federal mantém-se atenta às oportunidades e aos benefícios que podem trazer a internet e as redes sociais, mas, também, às ameaças e riscos presentes nos novos ambientes virtuais de relacionamento.

Nesse prisma, com a clara expectativa de que contribuirão para a segurança, o bem-estar, a harmonia e o respeito de toda a família policial militar, vem estabelecer recomendações gerais para o uso da internet e das redes sociais pelo efetivo da Polícia Militar do Distrito Federal – PMDF em serviço ou durante a folga.

II – OBJETIVOS

Estas recomendações têm por objetivo:

- 1) proporcionar à Polícia Militar e aos policiais militares angariarem os inúmeros benefícios disponíveis quando do uso da internet e das redes sociais;
- 2) orientar os policiais militares quanto aos cuidados e riscos de danos à reputação pessoal ou da Corporação pelo uso indevido ou descuidado da internet e das redes sociais;
- 3) orientar os policiais militares a fazerem o uso consciente e seguro da internet e das redes sociais durante o serviço ou nos períodos de folga;
- 4) evitar a exposição indevida de informações sensíveis relativas à PMDF, à segurança pública e a seus integrantes;
- 5) assegurar o adequado cumprimento do serviço policial militar; e
- 6) preservar a imagem institucional perante a sociedade.

III – ASPECTOS CONCEITUAIS RELEVANTES

a. A era da internet e as redes sociais

A internet trouxe inúmeras mudanças nas formas de interação e relacionamento interpessoal e institucional. A comunicação humana passou a ser articulada por meio da grande rede. As novas tecnologias proporcionaram a todos a possibilidade de expandir a capacidade de expressar e

divulgar suas opiniões, alcançando um público muito maior. Nesse contexto, a *web* e as redes de relacionamento virtual potencializaram essas relações, permitindo aos usuários:

- 1) fornecer informações pessoais;
- 2) acessar informações de terceiros;
- 3) utilizar mecanismos de comunicação;
- 4) agrupar-se, de acordo com afinidades, características, interesses e objetivos em comum; e
- 5) criar, gerenciar e compartilhar informações elaboradas, tais como páginas pessoais ou de divulgação temática ou comercial.

b. Atrativos e possibilidades

Por sua natureza, a internet e as redes sociais possuem muitos atrativos e oferecem diversas possibilidades de uso:

- 1) rapidez na propagação de informações;
- 2) expressiva quantidade de usuários;
- 3) acesso fácil;
- 4) grande disponibilidade de informações pessoais;
- 5) tempo ilimitado que as informações ficam disponíveis.

c. Principais vetores de risco

Também por sua natureza, a internet e as redes sociais ensejam inúmeros riscos, entre os quais são destacáveis:

- 1) invasões cibernéticas indesejadas ;
- 2) furtos de dados pessoais ;
- 3) contato com programas maliciosos (vírus, *malware*);
- 4) visita a conteúdos inapropriados ou ofensivos;
- 5) interação com pessoas mal intencionadas;
- 6) acesso a informações que podem ser usadas por criminosos para :
 - a) tentativas de sequestro;
 - b) furto de bens;
 - c) invasão de domicílio;
 - d) crimes diversos.
- 7) mal uso de informações;
- 8) prejuízos à imagem e à reputação;
- 9) vazamento e perda de informações.

d. As oito demandas prioritárias no uso das redes sociais

Tomando como referência todos os riscos ensejados pelo eventual uso displicente das redes sociais, é necessário que todo policial militar mantenha atenção constante e diligente sobre oito demandas prioritárias em relação ao uso da internet e das redes sociais:

- 1) Preservar sua privacidade;
- 2) Respeitar a privacidade alheia;
- 3) Proteger adequadamente seu computador e outros dispositivos de interação via *web*;
- 4) Proteger seu perfil pessoal;
- 5) Proteger sua família;
- 6) Proteger sua vida profissional;
- 7) Proteger o serviço policial militar; e
- 8) Proteger a Corporação.

e. Dicas relevantes sobre construção e uso de senhas eletrônicas

A senha é o um dos principais recursos de segurança constituindo-se como base de proteção pessoal e também organizacional.

Dessa forma, é essencial estabelecer senhas seguras, diferentes e nas quantidades necessárias ao seu dia-a-dia. Elas devem ser fortes e simples, contendo pelo menos 8 (oito) caracteres alfanuméricos e especiais, intercalando palavras e letras em caixa baixa e alta. Evite relacioná-las a preferência esportiva, religiosas, número de telefones, placas de veículos, datas natalícias ou qualquer outro tipo de informação que seja de fácil acesso ou dedução. Isso é importante, uma vez que os criminosos cibernéticos podem utilizar ferramentas capazes de obter acesso a sistemas, contas de e-mail e outros, através destas informações. Portanto, é fundamental a utilização de senhas seguras.

f. Alertas importantes

Perigos das contas e dos falsos perfis (*fakes*). As redes sociais proporcionam a possibilidade de se construir relacionamentos diversos: afetivos, profissionais, comerciais, etc. Tal gama de possibilidades pode expor o usuário a interagir com perfis ou contatos falsos. Algumas pessoas podem usar desses instrumentos para praticar ações criminosas ou levantamento de dados. No geral, eles agem para conquistar a confiança da vítima. Portanto, é conveniente evitar o contato com estranhos na rede.

Perigos da Engenharia Social. A Engenharia Social é a tentativa de espionagem que busca coletar informações e dados essenciais e confidenciais de pessoas ou instituições. Para isso, são utilizadas, na maior parte das vezes, informações oriundas de pessoas próximas como

cônjuges, pais, filhos, amigos e funcionários. Esse tipo de ação foi facilitada pela ampla utilização das redes sociais, pois além de reunir num mesmo ambiente textos, áudios, fotos, vídeos, planilhas, entre outros, permite aos engenheiros sociais o acesso a uma imensa quantidade de dados pessoais ou organizacionais.

Dessa forma, é importante evitar a postagem de fotos ou vídeos pessoais e familiares nas redes sociais. É importante, ainda, não revelar dados de bens ou de sua residência, uma vez que podem facilitar ações ilícitas, colocando em risco sua própria integridade física ou a de seus familiares.

IV – CONSIDERAÇÕES GERAIS

Estas recomendações têm por base as seguintes considerações gerais:

- 1) a liberdade constitucional à manifestação do pensamento (art. 5º, IV, CF/1988), bem como os limites à liberdade de expressão e a responsabilidade pelos seus atos;
- 2) a proteção constitucional à imagem e à honra das pessoas (art. 5º, X, CF/1988);
- 3) o crescimento exponencial do uso da internet e das redes sociais por toda a sociedade local e mundial;
- 4) os perigos decorrentes do uso das redes sociais aos próprios policiais militares, a seus familiares e, ainda, à instituição Polícia Militar do DF;
- 5) a necessidade de orientar os policiais militares da Corporação quanto às suas decisões e responsabilidades no uso da internet e das redes sociais durante o serviço ou no horário de folga;
- 6) a constante busca pelo aperfeiçoamento profissional do serviço policial militar prestado à sociedade e ao próprio público interno;
- 7) a possibilidade de informações divulgadas em redes sociais, ainda que inicialmente postadas em um grupo específico, virem ao conhecimento público, independentemente da vontade do usuário que efetuou a primeira postagem;
- 8) a expectativa da sociedade quanto ao policial militar como servidor de caráter íntegro, imparcial e que respeita os direitos humanos;
- 9) a possibilidade de descuido no uso da internet e das redes sociais pode gerar uma crise institucional por ato de um integrante da Corporação em razão da distorção de fato postado e da não confirmação da veracidade por parte dos usuários;
- 10) a tipificação dos crimes comuns e militares relacionados ao uso indevido dos símbolos da PMDF e às condutas ofensivas à hierarquia, à disciplina, à autoridade, bem como à imagem e à honra das pessoas;

- 11) a ética, a moral, a honra pessoal, o pundonor militar, o decoro da classe, os bons costumes, a urbanidade, o respeito e a harmonia entre os policiais militares.

V – CATEGORIAS ESPECIAIS DE RISCO

O uso seguro da internet e das redes sociais exige uma consciência dos riscos basicamente em cinco áreas:

- 1) violação da confiança ou do sigilo: divulgação de informação obtida por meio do serviço policial militar sobre a Corporação, o próprio serviço ou sobre os policiais militares;
- 2) violação não autorizada de dados pessoais: divulgação de informações pessoais sobre policiais militares ou terceiros;
- 3) descrédito sobre o serviço policial militar: atos em ou fora de serviço que afetem a confiança da sociedade na Corporação;
- 4) revelação de informações pessoais: grande vulnerabilidade a perseguição, corrupção ou extorsão;
- 5) revelação de táticas ou conteúdos operacionais: prejuízo às atividades policiais militares.

VI – ORIENTAÇÕES GERAIS

Ficam recomendadas as seguintes precauções gerais quando do uso da internet e das redes sociais:

- 1) os mesmos padrões de conduta, cuidados e comportamento no uso da internet e redes sociais devem ser aplicáveis quando o usuário estiver conectado ou não à internet;
- 2) todas as informações postadas na internet ou nas redes sociais devem ser consideradas como possíveis de serem divulgadas a um grande público;
- 3) evitar o uso da internet ou das redes sociais para assuntos de natureza particular utilizando equipamentos da Corporação ou, durante o serviço, utilizando equipamentos próprios como *smartphones*, *tablets* ou *notebooks*;
- 4) o uso de símbolos, uniformes, insígnias e imagens da Corporação são de caráter oficial e devem observar o previsto na legislação vigente, especialmente as disposições do Estatuto dos Policiais Militares da PMDF, do Manual de Identidade Visual da PMDF e no Regulamento de Uniformes da PMDF;

VII – ORIENTAÇÕES ESPECÍFICAS

a. Manutenção da confiança da sociedade

A sociedade perderá a confiança na Corporação se não tiver um grau mínimo de certeza de que as informações prestadas em caráter confidencial ou pessoal não serão divulgadas.

Nesse sentido, ficam recomendadas as seguintes precauções visando à manutenção da confiança da sociedade na PMDF:

- 1) o policial militar tem o dever funcional de não divulgar informações sobre terceiros obtidas em razão do serviço, sendo-lhe, portanto, proibida sua divulgação pela internet ou redes sociais;
- 2) as informações obtidas no serviço ou em razão do serviço não devem ser utilizadas para benefício pessoal nem divulgadas para terceiros, salvo quando, neste último caso, a função assim o exigir;
- 3) o policial militar não deve fazer comentários depreciativos contra a Corporação, seus superiores, pares, subordinados, contra o próprio serviço policial militar ou terceiros, em especial na internet ou nas redes sociais;
- 4) o policial militar deve utilizar os canais de comunicação oficiais ou aprovados pela Corporação para o encaminhamento de dados e informações do serviço.
- 5) todo policial militar tem a responsabilidade ética, moral, institucional e disciplinar de comunicar aos seus superiores qualquer irregularidade que afete a hierarquia, a disciplina, os preceitos institucionais, princípios e direitos fundamentais, a honra pessoal, o pundonor militar e/ou ao decoro da classe;
- 6) a manifestação do pensamento e a liberdade de expressão não podem ser confundidas com ofensas à hierarquia, à disciplina, à ética, à moral, aos bons costumes, à honra pessoal, ao pundonor militar e/ou decoro da classe;
- 7) a divulgação de documentos e informações institucionais somente poderá ocorrer se for devidamente autorizada.

b. Proteção aos dados pessoais e sensíveis

Dados pessoais sensíveis são os dados pessoais relativos às opiniões políticas, à crença religiosa ou a outras crenças da mesma natureza, à participação ou não de determinado grupo ou empresa, à saúde ou às condições física ou mental, à vida sexual, a procedimentos administrativos ou judiciais, a informações e imagens ridicularizadoras, ilegalmente obtidas ou que expõe pessoas a riscos diversos, entre outros aspectos relacionados à intimidade e à privacidade.

Ficam recomendadas as seguintes precauções visando à proteção aos dados pessoais e sensíveis:

- 1) ao policial militar que obtém dados pessoais sensíveis de terceiros durante o serviço ou em razão dele é expressamente proibido divulgá-los na internet, nas redes sociais ou em qualquer outro meio sem a devida autorização legal;
- 2) o policial militar é uma pessoa pública e deve ter a consciência de que, sempre que postar algo na internet ou redes sociais, o conteúdo poderá ser visto por seus superiores, pares, subordinados, familiares, vizinhos, amigos e outros.

c. Reputação da Polícia Militar do DF

A Polícia Militar do Distrito Federal reconhece que todo policial militar tem o direito constitucional à livre manifestação do pensamento e à liberdade de consciência e crença, todavia tais direitos possuem restrições mesmo no uso da internet e das redes sociais.

O policial militar pode não ser o porta-voz oficial da Corporação, porém, a partir do momento que se manifestar sobre algo relacionado à PMDF, à segurança pública, ao Governo ou a outros correlatos, poderá ser visto pelos demais usuários como alguém que fala em nome da instituição.

Considerando-se os dois parágrafos anteriores, ficam recomendadas as seguintes precauções quanto à reputação da Corporação ao se utilizar a internet e as redes sociais:

- 1) o descrédito no serviço policial militar pode ser consequência de um ato específico ou em razão da gradativa perda de confiança da população. Pela equidade, coerência e razoabilidade, o policial militar deve agir de modo a manter o respeito da população em todas as circunstâncias, e não somente quando houver cobertura da imprensa;
- 2) o policial militar deve estar sempre atento para o efeito propagador da internet e das redes sociais, vez que a informação mais simples pode assumir proporções superiores a todas as expectativas;
- 3) estando ou não de serviço, o policial militar deve manter uma conduta proba no uso da internet e das redes sociais;
- 4) o policial militar deve ter a consciência de que sua conduta, estando ou não de serviço, estará sujeita à apreciação administrativa disciplinar se macular a imagem da Corporação, a hierarquia, a disciplina, a ética, a moral, os bons costumes, a honra pessoal, o pundonor militar e/ou o decoro da classe policial militar;
- 5) não são toleráveis pontos de vista ou condutas que expressem ou apoiem discriminação contra qualquer pessoa ou grupo nem discriminações raciais, religiosas ou relacionadas à orientação sexual, ou quaisquer condutas contrárias ao esperado de um policial militar;

- 6) o policial militar deve ter consciência de que as postagens na internet ou nas redes sociais são diferentes da comunicação falada, podendo adquirir conotação diversa da pretendida. Na linguagem escrita das redes sociais é comum as pessoas não entenderem ironia, mensagens jocosas, humorísticas e também algumas referências particularizadas que elas desconhecem. Além disso, suas postagens são indexadas quase que instantaneamente por outras redes;
- 7) ao policial militar não é negado o direito de ter ou expressar sua opinião, mas deve ter a consciência de que é responsável pelos seus atos, gestos e palavras, e que suas manifestações poderão trazer-lhe consequências, positivas ou negativas.

d. Proteção à vida particular

Criminosos ou terceiros mal intencionados podem fazer uso da internet e das redes sociais para identificar informações pessoais sobre policiais militares com o objetivo de constranger, desacreditar, assediar, corromper ou chantageá-los ou seus familiares.

Os policiais militares que residem em zonas rurais, que prestam serviços em postos sensíveis, com nomes de guerra incomuns ou em postos de alto escalão estão particularmente mais vulneráveis a ataques por meio da internet ou redes sociais.

Considerando-se os dois parágrafos anteriores, ficam recomendadas as seguintes precauções visando à proteção da integridade do policial militar e de seus familiares ao se utilizar a internet e as redes sociais:

- 1) diante da possibilidade de ampla publicidade das informações e o potencial danoso de sua publicação, não convém ser postadas na internet ou nas redes sociais:
 - a) imagens fardado;
 - b) detalhes de seu perfil;
 - c) números de telefone celular ou fixo;
 - d) endereço residencial;
 - e) e-mails pessoais;
 - f) detalhes de membros da família;
 - g) locais onde costuma frequentar;
 - h) planos de viagens e períodos de ausência;
 - i) detalhes de veículos pessoais;
 - j) dados pessoais sensíveis;
 - k) detalhes de seu serviço;
 - l) imagens ou detalhes de colegas de trabalho sem sua ciência e consentimento;

- 2) considere sempre a real necessidade de qualquer postagem, pois, após a divulgação, não haverá como voltar atrás;
- 3) assegurar que suas configurações privadas nas redes sociais estejam no mais alto grau de privacidade;
- 4) não se registrar nas redes sociais utilizando e-mail institucional;
- 5) ser seletivo ao aceitar seus contatos ou “amigos” e estar atento às regras básicas de segurança ao permitir que seus “amigos” acessem seu perfil nas redes sociais;
- 6) não promover ou estar associado a materiais impróprios de perfis de “amigos” em redes sociais;
- 7) não fomentar ou estar associado a perfis nas redes sociais de criminosos ou contraventores penais;
- 8) não estar associado a perfis nas redes sociais de pessoas envolvidas em organizações criminosas;
- 9) ter ciência de que os usuários da internet podem não ser quem eles afirmam ser;
- 10) Utilizar senha de bloqueio nos dispositivos móveis (*tablets, smartphones, notebooks*), visto que costumam conter informações pessoais;
- 11) assegurar que computadores e *smartphones* tenham proteção contra *softwares* maliciosos;
- 12) manter seu computador seguro com todos os programas instalados nas versões mais recentes e com todas as atualizações aplicadas;
- 13) utilize e atualize sempre todos os mecanismos de segurança disponíveis, tais como *antispam, antimalware, firewall* pessoal;
- 14) seja cuidadoso ao acessar *links* reduzidos, utilizando complementos que permitam expandir o *link* antes de clicar nele;
- 15) usar senhas “fortes” e nunca compartilhá-las com terceiros, trocando-as periodicamente;
- 16) informar à Corporação, por meio de seu chefe imediato, caso seu perfil seja clonado, *hackeado* ou utilizado por terceiro não autorizado;
- 17) não divulgar eventos sociais relacionados ao serviço na internet ou nas redes sociais;
- 18) utilizar a intranet da PMDF para a divulgação das informações oficiais;
- 19) variar os locais utilizados para a realização de eventos sociais organizados por policiais militares.

- 20) avaliar cuidadosamente todos os riscos associados à utilização de contas pessoais nas redes sociais, em especial as informações referentes a seus familiares;
- 21) oriente seus filhos sobre todas essas precauções e outras que lhe parecerem pertinentes;
- 22) o policial militar que atue ou tenha a intenção de atuar em agências de inteligência deve considerar atentamente que a publicação de imagens e informações pessoais na internet e nas redes sociais podem eventualmente comprometer a sua atuação naquela área de ação policial.

e. Manutenção da segurança pública

A Polícia Militar tem o dever de prevenir e combater crimes e contravenções penais, prevenir e combater desordens, proteger comunidades vulneráveis e preservar os direitos humanos.

A manutenção ou não, bem como a divulgação ao público em geral de táticas e técnicas utilizadas no serviço policial militar, incluindo-se as sigilosas, compete ao Alto Comando da Corporação no interesse da segurança pública.

A divulgação de informações relacionadas a procedimentos apuratórios ou de pessoas envolvidas nesses procedimentos constituem violação do dever funcional do policial militar.

A divulgação não autorizada de operações, técnicas e táticas policiais podem acarretar sérias consequências para a segurança pública, podendo reduzir a eficácia e eficiência do serviço policial em geral bem como configurar uma infração penal militar.

Considerando-se os quatro parágrafos anteriores, ficam recomendadas as seguintes precauções visando à manutenção da segurança pública ao se utilizar a internet e as redes sociais:

- 1) é vedado ao policial militar divulgar operações, técnicas ou táticas policiais na internet ou nas redes sociais;
- 2) o policial militar deve atentar-se para o fato de que o acesso à internet de locais não confiáveis por meio de *notebooks*, *tablets*, *smartphones* ou similares pode involuntariamente permitir a divulgação de operações, técnicas ou táticas policiais que estejam armazenadas nesses dispositivos eletrônicos móveis;
- 3) ter ciência de que as fotos obtidas com *tablets* ou *smartphones* contêm dados que revelam a exata localização de onde foram obtidas e a subsequente postagem de tais fotos na internet ou redes sociais possibilita que informações pessoais ou funcionais sejam amplamente divulgadas, de modo não intencional, sem possibilidade de controle eficaz;
- 4) ter ciência de que os serviços de localização permitem que as redes sociais compartilhem com outros usuários a localização exata de determinado usuário,

dessa forma, terceiros podem ter acesso facilmente à identificação dos locais de trabalho, residencial e atual do usuário, por meio de padrões de deslocamento;

- 5) especialmente ao policial militar que atua na área de inteligência, é extremamente recomendável que desligue os serviços de localização e de GPS de seus *smartphones* e *tablets* com o fim de evitar a divulgação de sua localização quando postarem imagens ou fotos na internet e nas redes sociais;
- 6) o policial militar deve ter atenção especial ao habilitar o serviço de localização ou de GPS em seu *tablet* ou *smartphone* mesmo que sua utilização ocorra fora de serviço;
- 7) o policial militar deve ter cuidado com o conteúdo publicado nas redes sociais, evitando opiniões ofensivas a pessoas, empresas ou instituições, pois tais opiniões podem gerar crises institucionais ou ser enquadradas como criminosas.

f. Utilização dos símbolos da Polícia Militar do Distrito Federal

Os símbolos e o fardamento da PMDF possuem diversas disposições legais que regulamentam o seu uso e vedam diversas condutas. Dessa forma, ao utilizar os símbolos da PMDF na internet, bem como ao comercializar souvenirs através da rede de computadores, o policial militar deve atentar-se para os seguintes diplomas legais:

- 1) Estatuto dos Policiais Militares da Polícia Militar do Distrito Federal (Lei nº 7.289, de 18 de dezembro de 1984):

Art 70 - As prerrogativas dos policiais-militares são constituídas pelas honras, dignidade e distinções devidas aos graus hierárquicos e cargos.

Parágrafo único - São prerrogativas dos policiais-militares:

I - o uso de títulos, uniformes, distintivos, insígnias e emblemas da Polícia Militar, do Distrito Federal, correspondentes ao posto ou graduação;

Art 73 - Os uniformes da Polícia Militar com seus distintivos, insígnias e emblemas, são privativos dos policiais-militares e representam o símbolo da autoridade policial-militar, com as prerrogativas a ela inerentes.

Parágrafo único - Constituem crimes previstos na legislação específica o desrespeito aos uniformes, distintivos, insígnias e emblemas policiais-militares, bem como, seu uso por parte de quem a eles não tiver direito.

Art 74 - O uso dos uniformes com seus distintivos, insígnias e emblemas, bem como, os modelos, descrição, composição e peças acessórias, são estabelecidos em legislação peculiar da Polícia Militar do Distrito Federal.

Art 76 - É vedado a qualquer elemento civil ou organizações civis usar uniformes ou ostentar distintivos, insígnias ou emblemas que possam ser confundidos com os adotados na Polícia Militar.

Parágrafo único - São responsáveis pela infração das disposições deste artigo, além dos indivíduos que a tenham cometido, os Diretores ou Chefes de repartições, organizações de qualquer natureza, firma ou empregadores, empresas, institutos ou departamentos que tenham adotado ou consentido sejam usados uniformes ou ostentado distintivos, insígnias ou emblemas que possam ser confundidos com os adotados na Polícia Militar.

2) Lei nº 9.279, de 14 de maio de 1996 (Regula direitos e obrigações relativos à propriedade industrial):

Art. 191. Reproduzir ou imitar, de modo que possa induzir em erro ou confusão, armas, brasões ou distintivos oficiais nacionais, estrangeiros ou internacionais, sem a necessária autorização, no todo ou em parte, em marca, título de estabelecimento, nome comercial, insígnia ou sinal de propaganda, ou usar essas reproduções ou imitações com fins econômicos.

Pena - detenção, de 1 (um) a 3 (três) meses, ou multa.

Parágrafo único. Incorre na mesma pena quem vende ou expõe ou oferece à venda produtos assinalados com essas marcas.

3) Código Penal (Decreto-lei nº 2.848, de 7 de dezembro de 1940):

Falsificação do selo ou sinal público

Art. 296 - Falsificar, fabricando-os ou alterando-os:

I - selo público destinado a autenticar atos oficiais da União, de Estado ou de Município;

II - selo ou sinal atribuído por lei a entidade de direito público, ou a autoridade, ou sinal público de tabelião:

Pena - reclusão, de dois a seis anos, e multa.

§ 1º - Incorre nas mesmas penas:

I - quem faz uso do selo ou sinal falsificado;

II - quem utiliza indevidamente o selo ou sinal verdadeiro em prejuízo de outrem ou em proveito próprio ou alheio.

III - quem altera, falsifica ou faz uso indevido de marcas, logotipos, siglas ou quaisquer outros símbolos utilizados ou identificadores de órgãos ou entidades da Administração Pública. (Incluído pela Lei nº 9.983, de 2000)

§ 2º - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aumenta-se a pena de sexta parte.

4) Lei de Contravenções Penais (Decreto-lei nº 3.688, de 3 de outubro de 1941):

Art 46. Usar, publicamente, de uniforme, ou distintivo de função pública que não exerce; usar, indevidamente, de sinal, distintivo ou denominação cujo emprêgo seja regulado por lei. (Redação dada pelo Decreto-Lei nº 6.916, de 2.10.1944)

Pena – multa, de duzentos a dois mil cruzeiros, se o fato não constitui infração penal mais grave. (Redação dada pelo Decreto-Lei nº 6.916, de 2.10.1944)

5) Código Penal Militar (Decreto-lei nº 1.001, de 21 de outubro de 1969)

Art. 172. Usar, indevidamente, uniforme, distintivo ou insígnia militar a que não tenha direito:

Pena - detenção, até seis meses.

6) Regulamento Disciplinar do Exército (aplicado à PMDF pelo Decreto nº 23.317, de outubro de 25 de outubro de 2002)

Anexo I

Relação de transgressões

9. Deixar de cumprir prescrições expressamente estabelecidas no Estatuto dos Militares ou em outras leis e regulamentos, desde que não haja tipificação como crime ou contravenção penal, cuja violação afete os preceitos da hierarquia e disciplina, a ética militar, a honra pessoal, o pundonor militar ou o decoro da classe;

7) Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990)

Art. 66. Fazer afirmação falsa ou enganosa, ou omitir informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia de produtos ou serviços:

Pena - Detenção de três meses a um ano e multa.

§ 1º Incorrerá nas mesmas penas quem patrocinar a oferta.

§ 2º Se o crime é culposos;

Pena - Detenção de um a seis meses ou multa.

VIII – DISPOSIÇÕES FINAIS

A internet e as redes sociais podem oferecer e oferecem significativos benefícios aos policiais militares, mas trazem também muitos riscos.

A Polícia Militar do Distrito Federal encoraja seus policiais militares a extraírem o máximo desses benefícios, porém que o façam com responsabilidade e de forma a reduzir os riscos a níveis aceitáveis.

REFERÊNCIAS

- Constituição da República Federativa do Brasil de 1988.
- Código Penal. Decreto-Lei nº 2.848, [de 7 de dezembro de 1940](#).
- Código Penal Militar. Decreto-Lei nº 1.001, de [21 de outubro de 1969](#).
- Estatuto dos Policiais Militares da PMDF. Lei nº 7.289, de 18 de dezembro de 1984.
- *Guidelines on the safe use of the internet and social media by police officers and police staff, Associatiton of Chief Police Officers*.
- Manual de Conduta em Mídias Sociais, 1ª edição, 2012, da Empresa Brasileira de Pesquisa Agropecuária – Embrapa.
- Manual de Orientação para Atuação em Redes Sociais da Secretaria de Comunicação Social da Presidência da República, de outubro de 2012.
- Manual de Identidade Visual da Polícia Militar do Distrito Federal (MIV), aprovado pela Portaria PMDF nº 767, de 27 De Fevereiro De 2012.
- Segurança nas Redes Sociais. Cartilha. 1ª edição. Centro de Comunicação Social do Exército Brasileiro, 2013.