CONDUTA DIGITAL NAS FORÇAS ARMADAS

ANDRÉA VEIGA MARIN*
Capitão de Corveta (T)

SUMÁRIO

INTRODUÇÃO

No contexto das constantes transformações da sociedade moderna, verifica-se que as tecnologias de informação têm desempenhado importante papel, atuando como mola propulsora de uma verdadeira revolução comportamental, cujos elementos de difusão de informação tornaram-se itens indispensáveis e indissociáveis da rotina do indivíduo contemporâneo.

É inegável que a aderência maciça da sociedade aos apelos tecnológicos dos diversos recursos da comunicação digital vem alimentando uma dependência

* Graduada em Pedagogia, com habilitação em Educação de Jovens e Adultos, pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-graduada em Gestão de Educação à Distância, pela Universidade Federal Fluminense (UFF). Atualmente, serve na Diretoria do Patrimônio Histórico e Documentação da Marinha (DPHDM), na função de assistente do diretor.

crescente das redes sociais, condição esta que não apresenta, na mesma proporção e velocidade, mecanismos de equilíbrio e adequação de conduta dos usuários às boas práticas e ao uso ético das mídias digitais, configurando um ambiente fértil para ocorrências nocivas diretamente afetas às relações interpessoais e institucionais.

Na Figura 1, extraída do *site* G1 (GOMES, 2017), é exibido um gráfico contemplando dados do Instituto Brasileiro de Geografia e Estatística (IBGE), obtidos a partir da Pesquisa Nacional por Amostra de Domicílios (PNAD). Este gráfico mostra que o número de brasileiros que utilizam a internet ultrapassou os 100 milhões em 2015, evidenciando a velocidade expressiva do crescimento do número de internautas ao longo de quatro anos.

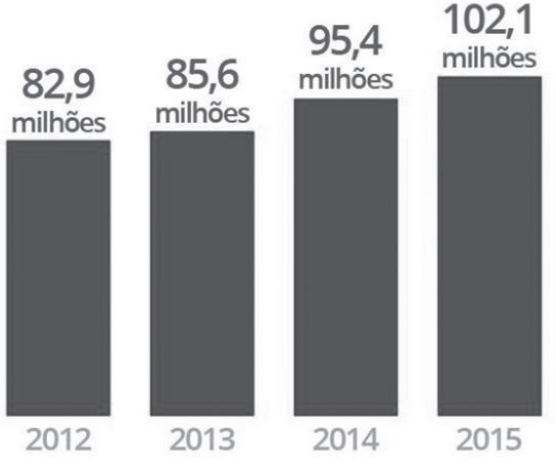

Figura 1 – População brasileira *online*
Fonte: Gomes (2017). G1. Elaborado em 24/11/2016

De acordo com dados disponibilizados pelo IBGE, o percentual de brasileiros que navegam na rede mundial de computadores subiu para 57% em 2015. A primeira vez que mais da metade da população brasileira se conectou à internet foi em 2014, ano em que o percentual de domicílios *online* chegou a 54,9% (GOMES, 2017).

Considerando essas transformações comportamentais em todos os níveis da sociedade, é natural que as organizações considerem relevante a adoção de programas e políticas internas que tenham como propósito uma ação conjunta permanente voltada para a orientação e formação de uma conduta digital ética e segura, a fim de que seus colaboradores e integrantes, dos mais variados escalões, sejam capazes de adotar boas práticas na utilização dos meios de comunicação digitais, na produção, transmissão ou compartilhamento de informações.

A necessidade de orientação de boas práticas digitais de comunicação surgiu a reboque das crescentes ocorrências de violações do direito privado e institucional no mundo virtual

A necessidade de orientação de boas práticas digitais de comunicação surgiu a reboque das crescentes ocorrências de violações do direito privado e institucional no mundo virtual. Em uma breve pesquisa pela internet, é possível verificar um significativo número de empresas que adotam um código próprio de conduta digital ou políticas internas rígidas de controle e mitigação de comportamentos reprováveis.

Neste contexto, surgiram também adequações e mudanças no âmbito forense. Atualmente, já podemos encontrar vasta literatura sobre o tema Direito Digital, cujo objetivo é propiciar uma interpretação diferenciada do Direito tradicionalmente conhecido, tendo como pano de fundo os fatos que agora ocorrem no âmbito virtual.

Várias são as iniciativas, produções acadêmicas, estudos e instrumentos legais que ratificam a importância do desenvolvimento de uma cultura de boas práticas e conduta digital. No entanto, ainda é comum a constante incidência de fatos envolvendo o mau uso das mídias e recursos remotos que são utilizados para divulgar, denegrir ou deturpar informações alheias, sejam elas pessoais ou institucionais.

Transmissão de informações tendenciosas e de fontes duvidosas, repasse de conteúdos proibidos e inadequados, ausência de filtros e análise crítica do usuário antes de registrar comentários, utilização e escolha equivocada de canais e meios digitais para envio de informações restritas e sigilosas, desconhecimento das tipificações relacionadas aos crimes virtuais aplicadas ao Código Civil e das consequências legais dessas infrações são alguns dos erros mais comuns cometidos por milhares de usuários.

Como prevenir inconvenientes ou prejuízos decorrentes do simples fato dos usuários das tecnologias de comunicação não adotarem hábitos e boas práticas digitais? Como mitigar os efeitos de condutas inadequadas dentro das instituições? Quais os caminhos para a construção de uma consciência digital ética e segura? Como prevenir danos à reputação e à imagem pessoal e institucional? No que tange a estas questões, é possível afirmar que as Forças Armadas (FA) estão atentas e vigilantes quanto aos delitos e excessos no uso das redes e mídias digitais. Instrumentos normativos e legislação específica, aplicáveis nos vários níveis hierárquicos, foram instituídos para mitigar as incidências de ocorrências do gênero (infração digital), a fim de coibir reincidências.

Os comportamentos distorcidos e desviados da finalidade original das plataformas e redes sociais, inicialmente destinadas à facilitação da comunicação para uso público entre grupos, pessoas e instituições, chamam a atenção por seu crescente potencial de influência e propagação. A ausência de elementos mediadores e filtros seguros para seleção e bloqueio de ações e acessos inadequados exigem dos usuários maior responsabilidade, reflexão e capacidade de discernir sobre sua conduta no ambiente *online* e, sobretudo, sobre os princípios e valores que irão norteá-la.

A Marinha dos Estados Unidos da América (United States Navy – USN), por exemplo, reconhece que as mídias sociais representam um dos principais modos de comunicação para os americanos e possuem um relevante potencial de propagação das informações que são compartilhadas. Assim, há uma preocupação permanente da Marinha norte-americana com os efeitos negativos que condutas inadequadas no ambiente virtual podem causar à instituição.

Um exemplo é o *blog* oficial da USN, mantido pelo Escritório de Informação da Marinha (Navy Office of Information/ Chief of U.S. Navy Information – Chinfo), página que se destina a fornecer informações e discussões atualizadas sobre a USN. Com o lema "Honra, Coragem, Compromisso *Online*, Todo o Tempo", o *blog*, entre inúmeras orientações, deixa claro que, uma vez que algum integrante da USN acesse uma plataforma de mídia social, ele ainda representa a USN (CHINFO, 2017a).

Em seu *Manual para Mídias Sociais* (CHINFO, 2017b), a USN apresenta uma série de recomendações normativas de procedimentos de segurança e padrões de liderança e conduta *online* para seus militares, seja em rotina operativa ou em sua vida pessoal. De acordo com o manual (CHINFO, 2017b), as mídias sociais representam um dos principais modos de comunicação para os americanos. Esse manual menciona que, a partir de 2011:

a) mais de 65% dos americanos usam redes sociais;

b) a cada semana no Facebook, mais de 3,5 bilhões de peças de conteúdo são compartilhadas;

c) um em cada quatro americanos vê um vídeo do YouTube diariamente; e

d) existem cerca de 245 milhões de usuários de internet no Estados Unidos da América (EUA).

Visando à proteção de informações críticas atinentes às operações militares, entre outras atividades, o manual (CHINFO, 2017b) apresenta as seguintes dicas-chave:

1) Proteja sua família, limitando a quantidade e tipo de informações que você publica sobre seus familiares, como nomes, endereços, cidades, locais ou escolas.

2) Compreenda cada uma das configurações de segurança da sua rede social, para que você possa tomar decisões sobre quem pode ou não visualizar suas informações e/ou fotos.

3) Mantenha as informações classificadas e sensíveis seguras, evitando discutir informações críticas, tais como movimentos de navios, operações militares, listas de pessoal e informações de armas.

4) Se você hesitar ao decidir se deve ou não compartilhar informações, não as publique *online*!

No âmbito da Marinha do Brasil (MB), há um rol normativo bastante abrangente e elucidativo no que diz respeito a esclarecimentos legais e regras de utilização, como, por exemplo, as Notas Técnicas (NT) da Diretoria de Comunicações e Tecnologia da Informação da Marinha – DCTIM, particularmente as NT nº 20/2002 (BRASIL. DCTIM, 2002), nº 10/2014 (BRASIL. DCTIM, 2014) e nº 14/2016 (BRASIL. DCTIM, 2016), além do Memorando nº 9/2016 do Comando de Operações Navais – ComOpNav (BRASIL. ComOpNav, 2016).

Contudo, mesmo com as claras definições legais disponibilizadas por meio de normas e regras internas e das orientações gerais deliberadas pelo Plano de Comunicação da Marinha, talvez possamos considerar que tais instrumentos normativos não se esgotam em seu próprio fim, havendo a necessidade de uma ação conjunta e contínua no sentido de estabelecer, gradativamente, uma consciência digital sólida e permanente.

O que justificaria esforços no sentido de implementar um Código de Conduta de Boas Práticas Digitais para Militares? Demandas internas de Organizações Militares (OM) específicas com a incidência de ocorrências pontuais não sinalizam uma motivação relevante para uma ação estratégica de caráter preventivo?

Não obstante as FA brasileiras possuírem respeitável reputação e credibilidade junto à população, cultivando cultura organizacional alicerçada em valores nobres e tradicionais, é mister voltarmos o olhar para o ambiente interno de nossas organizações, com o intuito de analisar de forma isenta nossos potenciais, fragilidades, erros e acertos, para que possamos atuar estrategicamente na preservação e manutenção institucional.

A partir do que foi exposto, delineamos o propósito do presente artigo, no sentido de sugerir ações que contribuam

para a disseminação e divulgação de boas práticas para conduta digital no âmbito militar. Para consecução deste propósito, foi realizada uma breve revisão da literatura a respeito do assunto e foram feitas citações de alguns casos reais de condutas inadequadas, que expomos a seguir.

REVISÃO DA LITERATURA

Direito Digital

Ao longo dos últimos dez anos, ocorreu um expressivo crescimento de publicações sobre o tema Direito Digital, com o propósito de oferecer mais informações sobre o devido tratamento legal de diversas situações originárias do ambiente virtual. Tal fato é decorrente da crescente demanda advinda da intensificação do uso de ambientes remotos de relacionamento (aplicativos, *chats*, redes sociais, *e-mails* etc.) e consequente aumento de ocorrências de práticas inadequadas no uso dos diversos recursos de comunicação digital.

Tanto em organizações privadas quanto governamentais, no Brasil e no mundo, o tema tem sido recorrentemente abordado. Como exemplo de iniciativa contemporânea no País, podemos citar a criação do Instituto Brasileiro de Direito Digital (IBDDIG), considerada uma *think tank* – organização que reúne profissionais, estudiosos e acadêmicos de determinada área a fim de difundir conhecimentos, conceitos estratégicos e descobertas relevantes sobre determinado tema, seja ele científico, político, social ou econômico –, que trabalha na investigação do assunto e fomenta estudos na área jurídica, trazendo ao público leigo informações relevantes em sua área de conhecimento e estudos (IBDDIG, 2017).

Casos Reais

É importante destacar que condutas inadequadas e equívocos no uso das mídias e recursos digitais independe de classe social, condição financeira, grau de escolaridade ou facilidades de acesso à informação e pode realmente ter consequências desastrosas.

Um exemplo na história recente é o caso da ex-candidata à Presidência dos EUA, a advogada Hillary Clinton. O caso, que ganhou repercussão internacional, refere-se à investigação conduzida pelo Departamento Federal de Investigação (Federal Bureau of Investigation – FBI) dos EUA, pelo fato da ex-primeira dama daquele país ter utilizado um servidor particular para o trâmite de informações confidenciais durante sua gestão como secretária de Estado dos EUA, de 2009 a 2013 (CHOZICK, 2016).

O fato foi revelado pela primeira vez em 2015 e voltou aos holofotes na reta final da disputa presidencial dos EUA, em novembro de 2016, quando o FBI anunciou que iria reabrir a investigação. Nesse fatídico episódio, rumores e comentários na imprensa norte-americana especularam sobre a forte influência negativa do ocorrido como justificativa para a derrota de Hillary Clinton nas urnas (CHOZICK, 2016).

Vários casos, não tão famosos, mas muito recorrentes, são registrados na internet e veiculados na mídia com frequência, configurando um vasto repertório de estudos de casos de condutas inadequadas a partir do uso de recursos remotos de comunicação digital e transmissão de informações e dados.

No País, quase diariamente, tomamos conhecimento de alguma situação constrangedora e com repercussões negativas, tanto de âmbito pessoal quan-

to institucional. Podemos citar como exemplo o caso envolvendo a Secretaria de Educação de um município do Estado do Rio de Janeiro, mencionado em reportagem veiculada por emissora de televisão, em que o áudio vazado de uma reunião continha comentário sugerindo a utilização de um jegue como meio de transporte para os professores daquela Rede Municipal de Ensino[1].

Outro caso citado em reportagem de emissora de televisão é o de uma médica que publicou em rede social as fotos do seu filho brincando de médico no centro cirúrgico. Na legenda de uma das fotos, a médica chama seu filho de doutor. Com luvas, máscara e avental da Santa Casa de Lagoa Santa, o garoto parece participar de cirurgia ao lado da mãe. A repercussão do caso provocou a demissão da cirurgiã.[2]

Em uma situação similar da área de saúde, uma médica foi demitida após fazer um comentário pejorativo, em sua rede social, sobre o nome da paciente que ela havia atendido: "Isso é um nome? Já imaginou quando ela era bebê?". A médica mostrou-se arrependida depois da repercussão do caso e comentou em entrevista: "Eu me arrependi logo após fazer a postagem. Um amigo meu, quando viu a postagem, disse: 'Tire logo isso daí por que vai repercutir mal'. Eu estou muito arrependida do que fiz. Não foi intencional para ofender a pessoa. Nada disso. Foi um comentário. Um comentário que foi indevido e infeliz".[3]

A partir dos fatos descritos, muitos podem se questionar sobre como essas pessoas, que protagonizaram situações tão constrangedoras, não tinham a noção de estarem sendo inconvenientes, imprudentes, antiéticas ou até mesmo cometendo um crime.

Percebemos uma ocasião conveniente e propícia para ações contundentes de reiteração da ética, da disciplina e da hierarquia, por meio de incrementos e adaptações doutrinárias na formação militar, com o objetivo de desenvolver o amadurecimento de uma conduta digital protetiva, preventiva e corretiva

Tais fatos revelam que o uso das redes sociais e meios de comunicação remotos criam automatismos tão perigosos que, em uma fração de segundos, o que podia parecer divertido ou um registro descontraído para compartilhar com amigos pode vir a ser interpretado e considerado algo comprometedor e passível de punições legais.

METODOLOGIA

Adotando um olhar mais crítico, no atual momento histórico e político que o País atravessa, percebemos uma ocasião conveniente e propícia para ações contundentes de reiteração da ética, da disciplina e da hierarquia, por meio de incrementos e adaptações doutrinárias na formação militar, com o objetivo de desenvolver o amadurecimento de uma conduta digital protetiva, preventiva e corretiva.

1 Reportagem do *Bom Dia Rio*, da Rede Globo de Televisão, exibida em 5 de junho de 2017.
2 Reportagem do *Jornal da Record*, da Rede Record de Televisão, exibida em 11 de maio de 2017.
3 Reportagem do *Jornal Fala Brasil*, da Rede Record de Televisão, exibida em 8 de junho de 2017.

Ação Protetiva

Há necessidade de ação protetiva na medida em que demanda orientações constantes acerca de procedimentos que visem à proteção do militar, sua integridade moral e psicológica, e institucional, no ambiente presencial ou virtual, corroborando para a manutenção da credibilidade da instituição, bem como seus valores e tradições, considerando que cada militar é um representante de sua respectiva Força.

Nesse aspecto, o clima organizacional deve favorecer à propagação dessas orientações a partir de vetores/agentes de liderança capazes de propagar bons exemplos e atitudes.

Ação Preventiva

A ação preventiva ocorre a partir de incrementos de conteúdos específicos sobre o tema, com prioridade para os cursos de formação em centros de instrução e escolas. Adestramentos permanentes nas OM, com estudos de casos e orientações quanto à adoção de boas práticas de comunicação digital (uso de redes sociais, compartilhamento de informações, critérios éticos para seleção de conteúdo, normas para construção de perfis seguros etc.) são reforços importantes para o processo de mudança comportamental.

Os estudos normativos e disciplinares e a ampla divulgação de legislação específica e das consequências disciplinares por ocasião da adoção de uma conduta digital inadequada também são ações que podem favorecer a internalização dos padrões de um novo comportamento digital.

Ação Corretiva

Como ação corretiva podemos ter, por exemplo, a elaboração de norma interna que tenha como propósito delinear um procedimento padrão para o tratamento de ocorrência de casos de conduta digital inadequada, sob a luz da legislação específica, que contemple inclusive deliberação em relação a alterações de procedimentos internos para a prevenção de novas ocorrências e divulgação das sanções aplicáveis.

PROCESSO

É importante destacar que o início de um trabalho educativo de amadurecimento da postura digital perpassa obrigatoriamente por um processo de mudança de comportamento. Tal mudança necessita de orientações progressivas e continuadas, as quais, a partir de um planejamento adequado, podem obter resultados observáveis em curto, médio e longo prazos.

Com caráter, predominantemente, educativo e preventivo, a proposta de desenvolvimento de uma cultura de boas práticas digitais possui similaridade com os programas de prevenção de acidentes, comumente empregados em setores operativos, como, por exemplo, a aviação. Nesse exemplo, o trabalho desenvolvido, para mitigação e controle dos fatores de risco, decorre de ações permanentes de supervisão e levantamento de ocorrências que alimentam uma análise estatística, cujo objetivo é avaliar o alcance positivo das ações preventivas.

Em um processo formativo, espera-se alcançar resultados qualitativos que influenciem tanto na manutenção de um ambiente organizacional salutar, ético e ordeiro quanto na difusão de hábitos e boas práticas digitais para além das OM, considerando que a conduta de cada militar é propagada em seu ciclo familiar e social.

CONSIDERAÇÕES FINAIS

Após a apreciação e análise dos argumentos expostos, podemos considerar que o tema "Conduta Digital" tem forte potencial e apelo para ser aproveitado e introduzido nas escolas e centros de instrução e formação de militares, abrangendo todos os níveis hierárquicos, podendo compor uma disciplina, dentro dos cursos de formação, ou constituir um curso expedito (presencial ou a distância), o que não demandaria, necessariamente, alteração curricular contundente.

Estrategicamente, esse processo deve ser conduzido, considerando metodologia que priorize a aprendizagem pragmática e com foco no desenvolvimento de competências comportamentais específicas para o propósito pretendido, em que as referências sobre conduta e práticas digitais são articuladas e confrontadas com as experiências e situações vivenciadas em diferentes momentos da rotina militar, favorecendo a internalização gradativa dos fundamentos norteadores de uma nova postura digital, mais isenta, madura e ética.

🗁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<EDUCAÇÃO>; Ensino; Comunicação; Formação; Ética; Conduta; Internet; Tecnologia da Informação;

REFERÊNCIAS

BRASIL. Comando de Operações Navais. Memorando nº 9 de 5 de setembro de 2013. Uso de *e-mail* e redes sociais por militares subordinados ao ComOpNav. Rio de Janeiro, 2016.

_____. Diretoria de Comunicações e Tecnologia da Informação da Marinha. Nota Técnica nº 20 de 9 de dezembro de 2002. Estudo sobre crimes de informática. Rio de Janeiro, 2002.

_____. _____. Nota Técnica nº 10 de 6 de fevereiro de 2014. Utilização de celular particular a bordo da OM. Rio de Janeiro, 2014.

_____. _____. Nota Técnica nº 14 de 9 de maio de 2016. Extrato de Normas que demonstram a existência legal que consideram como ilícito o vazamento de informações. Rio de Janeiro, 2016.

CHOZICK, Amy. "Hillary Clinton Blames F.B.I. Director for Election Loss". *The New York Times*, New York, 16 nov. 2016.

Chief of U.S. Navy Information. Navy Office of Information. Navy Live. The Offical Blog of the U.S. Navy. < http://navylive.dodlive.mil/>. Acesso em: 22 out. 2017a.

_____. _____. Navy Command Leadership Social Media Handbook. Disponível em: <http://www.navy.mil/ah_online/OPSEC/docs/Policy/>. Acesso em: 22 out. 2017b.

GOMES, Helton Simões. "Brasil supera marca de 100 milhões de internautas, diz IBGE". G1. Tecnologia e Games. São Paulo, 25 nov. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/11/>. Acesso em: 22 out. 2017.

Instituto Brasileiro de Direito Digital. Proteção dos Dados Pessoais, Privacidade, Inteligência Artificial (AI) e Investigação Cibernética. Disponível em: <http://www.ibddig.com.br/. Acesso em: 22 out. 2017.