

USO PESSOAL DE REDES SOCIAIS NO AMBIENTE DE TRABALHO: PRODUTIVIDADE, PRIVACIDADE, SEGURANÇA DA INFORMAÇÃO E DESAFIOS DE GESTÃO

SOARES, Miriam Rodrigues
RIBEIRO, Paula Vieira da Silva
BONFIM, Rosemeire Alves
OLIVEIRA, Stefanni Soares
Orientador: BARBOSA, Vitor Neves

Resumo

A consolidação das redes sociais e dos dispositivos móveis ampliou a conectividade dos trabalhadores e tornou mais tênues as fronteiras entre vida pessoal e atividade profissional. No ambiente corporativo, o uso pessoal dessas plataformas pode gerar distrações e interrupções, mas também pode funcionar como forma de breve recuperação, comunicação e manutenção de vínculos sociais. Este artigo analisa os impactos do uso pessoal de redes sociais no contexto laboral, com ênfase na produtividade, no comportamento organizacional, na privacidade do trabalhador, na segurança da informação e nas práticas de governança. O estudo foi desenvolvido por meio de pesquisa bibliográfica e documental, de abordagem qualitativa e caráter descritivo e exploratório. A discussão utiliza contribuições da gestão de pessoas, dos estudos sobre cyberloafing e uso de mídias sociais no trabalho, além da legislação brasileira de proteção de dados. A literatura indica que os efeitos das redes sociais não são uniformemente negativos: comportamentos excessivos e incompatíveis com as atividades podem reduzir foco e desempenho, ao passo que usos moderados ou associados ao trabalho podem contribuir para engajamento, compartilhamento de conhecimento e recuperação da atenção. Verifica-se ainda que políticas de controle devem observar proporcionalidade, transparência, finalidade e necessidade, especialmente quando envolvem tratamento de dados pessoais. Conclui-se que a gestão eficaz não deve basear-se apenas na proibição ou na vigilância, mas na combinação de regras claras, educação digital, segurança da informação, liderança, definição de responsabilidades e monitoramento proporcional aos riscos.

Palavras-chave: Redes Sociais; Produtividade; Cyberloafing; Privacidade; Segurança da Informação.

Introdução

As redes sociais passaram a ocupar posição central na vida cotidiana e, conseqüentemente, também ingressaram de maneira permanente no ambiente de trabalho. Smartphones, aplicativos de mensagens e plataformas digitais permitem que o trabalhador mantenha contatos pessoais durante o expediente, acompanhe notícias, participe de comunidades,

produza conteúdo e acesse serviços sem depender da infraestrutura tecnológica da empresa. Essa realidade torna insuficiente uma abordagem de gestão baseada apenas no bloqueio de sites ou na restrição do acesso à internet.

O projeto que deu origem a este artigo formulou como problema de pesquisa a necessidade de compreender o impacto do uso excessivo de redes sociais pessoais sobre a produtividade dos colaboradores. Também apontou um dilema relevante: de um lado, o uso inadequado pode comprometer concentração, segurança e clima organizacional; de outro, políticas excessivamente rígidas de monitoramento podem afetar privacidade e confiança.

Lupianhes (2017) aborda a influência das redes sociais sobre as interações dos trabalhadores e destaca o caráter ambivalente dessas ferramentas no contexto organizacional. As mídias digitais podem favorecer comunicação e conectividade, mas também criam desafios relacionados ao foco, à gestão do tempo e à delimitação entre interesses pessoais e profissionais.

Na literatura internacional, o uso da internet da organização para atividades pessoais durante o horário de trabalho passou a ser estudado sob o conceito de cyberloafing. Lim (2002) descreve o fenômeno como o uso voluntário da internet da empresa para finalidades não relacionadas ao trabalho durante o expediente. Com o avanço dos smartphones e das redes móveis, o conceito deixou de depender exclusivamente da infraestrutura corporativa e passou a representar um comportamento digital mais amplo.

A discussão atual mostra, entretanto, que o impacto do uso pessoal da internet não é linear. Coker (2011) identificou efeitos positivos associados a formas moderadas de navegação pessoal durante o trabalho, sugerindo que pequenas pausas digitais podem contribuir para recuperação da concentração. Lim e Teo (2024), em revisão da literatura sobre cyberloafing, também destacam que o fenômeno apresenta antecedentes e consequências variados, não sendo adequado classificá-lo de maneira automática como comportamento necessariamente destrutivo.

A distinção entre uso pessoal e uso profissional também é importante. Zhao et al. (2021) observaram que o uso de mídias sociais voltado ao trabalho pode favorecer engajamento e desempenho, demonstrando que a tecnologia social pode atuar como recurso organizacional quando integrada a objetivos profissionais. Assim, o problema de gestão não consiste na existência das redes sociais em si, mas na forma como seu uso se relaciona às tarefas, às normas, à segurança e aos resultados esperados.

Além da produtividade, o tema envolve direitos e responsabilidades. No Brasil, a Lei Geral de Proteção de Dados Pessoais - LGPD estabelece princípios como finalidade, adequação, necessidade, transparência e segurança no tratamento de dados pessoais (BRASIL, 2018). Esses princípios são relevantes quando empresas adotam ferramentas de monitoramento, registros de acesso, filtros de conteúdo ou mecanismos de análise comportamental.

Diante desse cenário, o objetivo geral deste artigo é analisar diretrizes para a gestão do uso pessoal de redes sociais no ambiente corporativo, buscando conciliar produtividade, segurança da informação e respeito à privacidade do trabalhador. Como objetivos específicos, pretende-se discutir impactos sobre desempenho e comportamento organizacional, examinar riscos de segurança e reputação, analisar limites relacionados ao monitoramento e propor práticas de governança adequadas à realidade digital.

Metodologicamente, trata-se de pesquisa bibliográfica e documental, de abordagem qualitativa e caráter descritivo e exploratório. Foram considerados livros, artigos científicos e documentos legais relacionados à gestão de pessoas, cyberloafing, mídias sociais no trabalho, produtividade, privacidade, monitoramento e proteção de dados. A opção pela pesquisa bibliográfica decorre da ausência, no projeto original, de levantamento de campo ou base estatística própria.

1. Redes sociais, conectividade e transformação do ambiente de trabalho

A transformação digital modificou não apenas os instrumentos de produção, mas também a forma como os trabalhadores se comunicam e administram sua vida cotidiana. A mesma tecnologia utilizada para acessar sistemas empresariais permite interações pessoais em tempo real, tornando mais difícil separar de maneira absoluta o espaço digital profissional do espaço digital privado.

Chiavenato (2014) destaca que a gestão de pessoas precisa acompanhar mudanças tecnológicas e comportamentais que afetam as organizações. Nessa perspectiva, novas tecnologias não devem ser analisadas apenas como ferramentas técnicas, pois alteram relacionamentos, expectativas, formas de controle, processos de aprendizagem e práticas de comunicação.

Lupianhes (2017) observa que as redes sociais estão incorporadas à cultura contemporânea e influenciam a interação entre trabalhadores. Essa característica explica por que

políticas que simplesmente pressupõem a eliminação do uso pessoal tendem a enfrentar dificuldades práticas. Em muitos casos, o trabalhador utiliza o mesmo dispositivo para autenticação de serviços profissionais, comunicação com familiares, transporte, operações bancárias e interação em redes sociais.

A conectividade permanente também produz benefícios para as organizações. Plataformas sociais podem facilitar o compartilhamento rápido de informações, a criação de redes profissionais, a busca de conhecimento e a comunicação entre pessoas geograficamente distantes. Zhao et al. (2021) demonstram que o uso de mídias sociais voltado ao trabalho pode favorecer o engajamento e diferentes dimensões do desempenho profissional.

Ao mesmo tempo, a presença contínua de notificações, mensagens e conteúdos personalizados amplia a concorrência pela atenção do trabalhador. A questão gerencial, portanto, não pode ser formulada apenas como uma oposição entre acesso e bloqueio. É necessário compreender frequência, duração, finalidade, contexto da função e impacto efetivo sobre a entrega.

Essa abordagem permite distinguir usos funcionais, usos pessoais moderados e comportamentos excessivos. Sem essa diferenciação, a empresa corre o risco de tratar atividades distintas da mesma forma e criar políticas desproporcionais, incapazes de reconhecer tanto os riscos quanto os possíveis benefícios da conectividade.

2. Cyberloafing, distração e produtividade

O conceito de cyberloafing tornou-se uma das principais referências para analisar o uso pessoal da internet durante o trabalho. Lim (2002) investigou esse comportamento no contexto organizacional e demonstrou que sua ocorrência também se relaciona à percepção de justiça e às formas utilizadas pelos trabalhadores para justificar o uso pessoal da internet.

Blanchard e Henle (2008) demonstram que o cyberloafing pode assumir diferentes formas e intensidades. Algumas práticas são consideradas de menor gravidade, como consultas rápidas a conteúdos pessoais, enquanto outras podem envolver atividades mais prolongadas ou incompatíveis com as responsabilidades do cargo. Essa distinção é fundamental para políticas internas proporcionais.

O impacto sobre a produtividade depende de elementos como frequência, duração, complexidade da função e momento em que a interrupção ocorre. Atividades que exigem

concentração contínua podem ser mais sensíveis a interrupções do que tarefas com períodos naturais de espera ou alternância. Assim, medir apenas o tempo de acesso a uma plataforma não necessariamente explica a qualidade da entrega profissional.

O uso excessivo pode fragmentar a atenção, prolongar a conclusão de tarefas e aumentar a necessidade de retomada cognitiva após cada interrupção. Além disso, quando atividades pessoais ocupam parte significativa do expediente, podem ocorrer atrasos, transferência de carga para colegas e percepção de injustiça dentro da equipe.

Entretanto, a literatura também recomenda cautela com conclusões absolutas. Coker (2011) observou efeitos positivos relacionados a formas moderadas de navegação pessoal durante a jornada, associadas a pequenas pausas e recuperação da concentração. Isso sugere que breves intervalos digitais podem cumprir função semelhante à de outras pausas informais.

Lim e Teo (2024), ao revisarem a produção sobre cyberloafing, evidenciam que o fenômeno pode produzir consequências positivas ou negativas, conforme as circunstâncias. Portanto, a gestão deve concentrar-se em comportamentos que efetivamente interferem nas responsabilidades profissionais, em vez de presumir que qualquer acesso pessoal representa perda automática de produtividade.

Uma política equilibrada pode adotar critérios ligados ao resultado, à responsabilidade e ao risco. Funções críticas, ambientes regulados e atividades que envolvem atendimento contínuo podem exigir limites mais rigorosos; em outros contextos, pequenas utilizações pessoais podem ser administradas sem prejuízo significativo ao desempenho.

3. Redes sociais, comportamento organizacional e normas de equipe

O comportamento digital no trabalho não é determinado exclusivamente por escolhas individuais. Normas sociais, exemplos de liderança e práticas da equipe influenciam a percepção sobre o que é considerado aceitável. Quando regras formais e comportamentos reais são contraditórios, aumenta a ambiguidade e diminui a efetividade das políticas.

Blanchard e Henle (2008) identificaram relações entre normas percebidas e diferentes formas de cyberloafing. Isso significa que o colaborador observa a conduta de colegas e superiores para compreender os limites informais do ambiente. Se gestores utilizam redes pessoais de maneira constante durante reuniões, por exemplo, torna-se mais difícil sustentar uma regra de proibição absoluta para os demais.

Chiavenato (2014) ressalta a importância da cultura e das práticas de gestão de pessoas para alinhar comportamentos aos objetivos organizacionais. Políticas de uso de tecnologia precisam, portanto, ser acompanhadas por comunicação coerente, liderança e critérios aplicáveis aos diferentes níveis da organização.

A percepção de justiça também interfere na adesão às regras. Restrições que parecem arbitrárias, seletivas ou aplicadas apenas a determinados grupos podem reduzir confiança. Em contrapartida, normas explicadas a partir de riscos concretos, responsabilidades funcionais e segurança tendem a ser mais compreensíveis.

As redes sociais ainda afetam relações interpessoais internas. Postagens, comentários, grupos privados e compartilhamentos podem gerar conflitos que ultrapassam o ambiente digital e chegam ao trabalho. Por isso, ações educativas sobre convivência, respeito, confidencialidade e reputação são tão importantes quanto medidas técnicas.

A gestão do comportamento organizacional no ambiente digital exige clareza sobre a diferença entre opinião pessoal e representação institucional. Trabalhadores precisam compreender quando estão utilizando perfis oficiais, quando atuam como representantes da empresa e quais cuidados devem adotar ao divulgar informações obtidas em razão de suas funções.

4. Benefícios do uso profissional e necessidade de diferenciação

A presença das redes sociais no trabalho não pode ser analisada apenas a partir de riscos. Muitas organizações utilizam plataformas sociais para comunicação, recrutamento, marketing, relacionamento com clientes, aprendizagem e compartilhamento de conhecimento. Nesses casos, o acesso às redes integra a própria atividade profissional.

Zhao et al. (2021) verificaram que o uso de mídias sociais baseado no trabalho pode aumentar o engajamento, que por sua vez se relaciona positivamente a dimensões do desempenho. O estudo reforça a necessidade de distinguir o uso profissional do uso pessoal, evitando políticas genéricas que prejudiquem atividades produtivas.

A mesma plataforma pode desempenhar funções diferentes. Um empregado pode utilizar uma rede para acompanhar tendências do setor durante parte do tempo e, em outro momento, acessar conteúdo exclusivamente pessoal. Por isso, ferramentas automáticas de bloqueio ou de classificação nem sempre conseguem interpretar adequadamente a finalidade do acesso.

Também existem usos pessoais que podem produzir efeitos indiretos positivos, como resolver rapidamente uma questão familiar e retornar à tarefa com menor preocupação. Coker (2011) associa o uso moderado da internet para lazer a mecanismos de recuperação da atenção. Isso não significa que toda atividade pessoal aumente produtividade, mas indica que a relação não é simplesmente proporcional ao tempo de acesso.

A diferenciação entre uso funcional, uso pessoal moderado e uso abusivo permite uma política mais racional. Critérios podem considerar impacto na entrega, interrupção de serviços, risco de segurança, exposição de dados, reincidência e descumprimento de orientações previamente comunicadas.

Esse modelo substitui a lógica de vigilância permanente por uma abordagem de governança. O objetivo deixa de ser controlar cada minuto de navegação e passa a ser assegurar que a conectividade seja compatível com responsabilidades, ética, segurança e resultados.

5. Privacidade, monitoramento e LGPD

O monitoramento tecnológico no ambiente de trabalho representa um dos pontos mais sensíveis do tema. As organizações possuem interesses legítimos relacionados à proteção de ativos, segurança, continuidade das atividades e verificação do uso de recursos corporativos. Entretanto, o exercício de controle não elimina os direitos fundamentais de privacidade e proteção de dados do trabalhador.

A Lei Geral de Proteção de Dados Pessoais estabelece que o tratamento de dados deve observar, entre outros, os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização (BRASIL, 2018). Em termos de gestão, isso significa que a empresa deve ser capaz de explicar por que coleta determinado dado, para qual finalidade, por quanto tempo e em que medida a coleta é necessária.

O princípio da necessidade é especialmente relevante para ferramentas de monitoramento. Se determinado objetivo pode ser alcançado por uma medida menos invasiva, a coleta excessiva de informações pessoais pode ser incompatível com uma política baseada em minimização de dados. Da mesma forma, a transparência exige que trabalhadores recebam informações claras sobre práticas de tratamento aplicáveis.

A jurisprudência trabalhista brasileira já discutiu o monitoramento de recursos corporativos. Em comunicação institucional de 2017, o Tribunal Superior do Trabalho relatou

decisão que admitiu, naquele caso, o monitoramento de e-mail corporativo fornecido pelo empregador, sem considerar configurada violação à intimidade. Essa compreensão, contudo, não deve ser generalizada como autorização irrestrita para monitorar contas pessoais ou toda a atividade digital do empregado.

Redes sociais pessoais apresentam características distintas do e-mail corporativo. O fato de determinado conteúdo estar acessível publicamente não transforma qualquer tratamento posterior em automaticamente legítimo ou ilimitado. A LGPD determina que o tratamento de dados deve respeitar finalidade, boa-fé e os direitos do titular, inclusive quando informações tiverem sido tornadas públicas.

Assim, políticas de monitoramento devem priorizar recursos corporativos, riscos objetivos e dados necessários à finalidade. A empresa também deve diferenciar segurança de conteúdo, produtividade e investigação disciplinar, evitando sistemas de vigilância genéricos que coletem informações sem relação clara com as atividades profissionais.

Do ponto de vista de confiança organizacional, a transparência possui valor adicional. Trabalhadores que conhecem as regras e os limites do monitoramento conseguem ajustar seus comportamentos e compreender as responsabilidades envolvidas. O controle secreto ou excessivamente intrusivo tende a gerar insegurança e resistência.

6. Segurança da informação, confidencialidade e risco reputacional

O uso de redes sociais no trabalho também se relaciona diretamente à segurança da informação. Publicações aparentemente informais podem revelar dados de clientes, documentos, imagens de telas, rotinas internas, localização, projetos, credenciais ou informações estratégicas.

A LGPD determina que agentes de tratamento adotem medidas técnicas e administrativas aptas a proteger dados pessoais contra acessos não autorizados, perda, alteração, comunicação ou tratamento inadequado (BRASIL, 2018). Essa obrigação reforça a necessidade de integrar políticas de redes sociais aos programas de segurança e proteção de dados.

A prevenção não depende apenas de bloqueios tecnológicos. Muitos incidentes decorrem de comportamento humano: compartilhamento indevido, engenharia social, utilização de senhas fracas, exposição de documentos em fotografias e interação com perfis fraudulentos. Por essa razão, conscientização contínua é componente essencial da governança.

Outro risco envolve a reputação institucional. Postagens de empregados podem ser associadas à organização, especialmente quando o perfil identifica o vínculo profissional. É necessário, entretanto, diferenciar manifestação pessoal legítima de situações concretas que exponham informações confidenciais, utilizem indevidamente a marca ou produzam riscos diretamente vinculados à atividade profissional.

Políticas internas devem explicar exemplos de informação protegida, responsabilidades sobre imagens de ambiente de trabalho, uso de logotipos, divulgação de clientes, registros de reuniões e publicações em eventos internos. Quanto mais concretas forem as orientações, menor a dependência de interpretações subjetivas.

A segurança da informação deve ser vista como responsabilidade compartilhada. A empresa deve oferecer infraestrutura adequada, controles proporcionais e treinamento, enquanto o colaborador precisa respeitar as regras de confidencialidade e utilizar os recursos de forma responsável.

7. Boas práticas de governança para o uso de redes sociais

A análise da literatura e da legislação permite propor um conjunto de boas práticas para gestão do uso pessoal de redes sociais. A primeira delas é estabelecer uma política clara, acessível e compatível com as atividades reais. Regras excessivamente genéricas ou absolutas são difíceis de aplicar e podem desconsiderar funções nas quais o uso de redes integra o trabalho.

A política deve diferenciar dispositivos e contas corporativas de dispositivos e contas pessoais. Também deve explicar quais registros podem ser coletados em equipamentos da organização, quais finalidades justificam a coleta e quais medidas de segurança são utilizadas.

Outro princípio é a proporcionalidade. Pequenos acessos pessoais que não prejudiquem o serviço não devem necessariamente receber o mesmo tratamento de comportamentos repetitivos que interfiram em prazos, atendimento ou segurança. A gradação de respostas favorece coerência e justiça.

A liderança precisa ser preparada para administrar o tema sem transformar cada ocorrência em conflito disciplinar. O gestor deve avaliar impacto efetivo, contexto, reincidência e clareza das regras existentes. Antes de medidas punitivas, muitas situações podem ser corrigidas por orientação e alinhamento de expectativas.

Programas de letramento digital devem incluir produtividade, segurança, proteção de dados, engenharia social, reputação e convivência. A educação permite que o colaborador compreenda não apenas o que é proibido, mas por que determinados comportamentos criam riscos.

Indicadores de desempenho também devem ser utilizados de maneira cuidadosa. A organização pode acompanhar entregas, qualidade, prazos e resultados em vez de presumir produtividade a partir do simples tempo de conexão. Essa mudança reduz incentivos à vigilância excessiva e aproxima a avaliação daquilo que efetivamente importa para a atividade.

Quando o monitoramento for necessário, a coleta deve ser limitada ao mínimo adequado à finalidade, respeitando os princípios da LGPD. Informações sobre práticas de monitoramento devem integrar políticas internas e avisos de privacidade aplicáveis aos trabalhadores.

Finalmente, a política precisa ser revisada periodicamente. Novas plataformas, inteligência artificial, trabalho híbrido, dispositivos pessoais e mudanças legislativas alteram continuamente o cenário. Governança digital exige atualização, diálogo entre gestão de pessoas, tecnologia, segurança, jurídico e liderança.

Considerações Finais

O uso pessoal de redes sociais no ambiente de trabalho constitui um fenômeno complexo e não pode ser adequadamente administrado por meio de uma lógica exclusivamente proibitiva. A transformação digital tornou a conectividade parte da rotina dos trabalhadores, aproximando atividades profissionais e pessoais e exigindo novas formas de gestão.

O problema central do projeto questionava o impacto do uso excessivo de redes sociais sobre a produtividade. A literatura analisada confirma que comportamentos digitais podem produzir distrações, interrupções e perda de foco quando são frequentes, prolongados ou incompatíveis com as responsabilidades da função. Entretanto, também demonstra que usos moderados e breves podem funcionar como pausas de recuperação e que o uso profissional das redes sociais pode favorecer comunicação, engajamento e compartilhamento de conhecimento.

A contribuição dos estudos sobre cyberloafing é justamente mostrar que diferentes comportamentos precisam ser analisados de forma distinta. Lim (2002), Blanchard e Henle (2008), Coker (2011) e Lim e Teo (2024) permitem compreender que intensidade, finalidade, normas sociais e contexto organizacional influenciam os efeitos do uso pessoal da internet.

No campo da gestão de pessoas, a coerência das regras e o comportamento da liderança são fundamentais. Políticas que proíbem determinadas práticas, mas são ignoradas por gestores ou aplicadas de maneira seletiva, tendem a perder legitimidade. A organização precisa alinhar normas formais, cultura e critérios de avaliação.

Outro ponto central é a privacidade. A existência do poder de direção e de interesses empresariais legítimos não significa ausência de limites para o tratamento de dados dos empregados. A LGPD introduz parâmetros importantes de finalidade, necessidade, transparência, segurança e responsabilização que devem orientar iniciativas de monitoramento.

A segurança da informação amplia a relevância do tema. Redes sociais podem ser utilizadas como vetores de engenharia social e também podem facilitar exposição involuntária de dados, documentos, imagens e informações estratégicas. Por isso, proteção tecnológica deve ser acompanhada por educação digital e políticas claras de confidencialidade.

Conclui-se que a estratégia mais adequada combina definição de responsabilidades, regras proporcionais, comunicação transparente, formação de líderes, letramento digital, gestão por resultados e medidas de segurança. O objetivo não deve ser eliminar a conectividade pessoal, mas assegurar que ela permaneça compatível com produtividade, direitos individuais e proteção dos ativos organizacionais.

Como limitação, este artigo possui natureza bibliográfica e documental e não mede diretamente o tempo de uso de redes sociais ou a produtividade de trabalhadores de uma organização específica. Estudos futuros podem combinar registros de uso, indicadores de desempenho e entrevistas, respeitando requisitos éticos e de proteção de dados, para identificar relações entre comportamento digital, contexto de trabalho e resultados.

Referências

BLANCHARD, Anita L.; HENLE, Christine A. Correlações entre diferentes formas de cyberloafing: o papel das normas e do locus de controle externo. *Computers in Human Behavior*, v. 24, n. 3, p. 1067-1084, 2008. DOI: 10.1016/j.chb.2007.03.008.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 12 ago. 2026.

CHIAVENATO, Idalberto. Gestão de pessoas: o novo papel dos recursos humanos nas organizações. 4. ed. Barueri: Manole, 2014.

COKER, Brent L. S. Liberdade para navegar: os efeitos positivos da navegação de lazer na internet durante o trabalho. *New Technology, Work and Employment*, v. 26, n. 3, p. 238-247, 2011. DOI: 10.1111/j.1468-005X.2011.00272.x.

LIM, Vivien K. G. A forma digital de se distrair no trabalho: cyberloafing, neutralização e justiça organizacional. *Journal of Organizational Behavior*, v. 23, n. 5, p. 675-694, 2002. DOI: 10.1002/job.161.

LIM, Vivien K. G.; TEO, Thompson S. H. Cyberloafing: revisão e agenda de pesquisa. *Applied Psychology*, v. 73, n. 1, p. 441-484, 2024. DOI: 10.1111/apps.12452.

LUPIANHES, Karen. A influência das redes sociais no ambiente de trabalho: como o advento das redes sociais influencia o modo de interagir dos trabalhadores. [S. l.]: Novas Edições Acadêmicas, 2017. ISBN 9783330202948.

TRIBUNAL SUPERIOR DO TRABALHO. Pode ou não pode: o empregador monitorar e-mail corporativo de trabalhadores? Brasília, DF: TST, 13 jul. 2017. Disponível em: <https://www.tst.jus.br/-/pode-ou-nao-pode-o-empregador-monitorar-e-mail-corporativo-de-trabalhadores>. Acesso em: 12 ago. 2026.

ZHAO, Junzhe et al. O impacto positivo do uso de mídias sociais baseado no trabalho sobre o desempenho profissional. *International Journal of Environmental Research and Public Health*, v. 18, n. 21, art. 11578, 2021. DOI: 10.3390/ijerph182111578.