

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian, kebijakan formatif terhadap tindak pidana *doxing* di Indonesia saat ini (*ius constitutum*) masih belum memberikan pengaturan yang tegas, eksplisit, dan komprehensif. Meskipun terdapat ketentuan dalam UUD 1945, UU ITE, UU PDP, dan sebagian dalam KUHP, namun keseluruhannya belum mengakui *doxing* sebagai tindak pidana yang berdiri sendiri. Pasal-pasal yang ada masih bersifat umum, multitafsir, dan tidak mengatur unsur-unsur delik *doxing* secara rinci, baik dari segi motif, bentuk, maupun akibat hukumnya. Akibatnya, penegakan hukum terhadap pelaku *doxing* masih lemah, tidak konsisten, dan kurang mampu memberikan perlindungan hukum yang maksimal bagi korban.

Dalam aspek pertanggungjawaban pidana, hukum positif Indonesia belum membedakan secara jelas antara *doxing* yang dilakukan dengan kesengajaan (*dolus*) dan kelalaian (*culpa*). Akibatnya, tidak ada perbedaan dalam pemberian sanksi, sehingga pelaku yang secara tidak sengaja menyebarkan data pribadi dapat dikenai sanksi yang sama dengan pelaku yang secara sadar dan jahat melakukan *doxing*. Sementara itu, sanksi pidana dalam UU PDP pun masih terbatas dan belum mencerminkan derajat keparahan atau dampak dari masing-masing jenis *doxing*. Perlindungan terhadap korban juga belum menjadi fokus utama dalam regulasi saat ini, padahal dampak psikologis, sosial, dan fisik dari *doxing* sangat signifikan.

Sebagai respons terhadap kekosongan hukum ini, dalam perspektif *ius constituendum*, Indonesia perlu merumuskan kebijakan hukum pidana yang lebih progresif, spesifik, dan preskriptif mengenai tindak pidana *doxing*. Rumusan ini dapat mengacu pada sistem hukum Singapura yang telah mengatur *doxing* secara eksplisit melalui *Protection from Harassment Act (POHA) 2019*, yang tidak hanya mengkategorikan berbagai bentuk *doxing* (targeting, delegitimizing, dan deanonymizing), tetapi juga mengatur sanksi pidana yang proporsional, pertanggungjawaban yang diferensial, dan mekanisme perlindungan korban yang proaktif. Kebijakan semacam ini dapat diintegrasikan dalam revisi UU PDP, penguatan UU ITE, atau bahkan pembentukan undang-undang khusus tentang kejahatan privasi berbasis digital.

Dengan adanya kebijakan formulatif yang terstruktur dan berpandangan ke depan, Indonesia akan mampu menjawab tantangan perkembangan kejahatan siber, khususnya *doxing*. Pengaturan yang jelas dan adaptif akan memberikan kepastian hukum bagi aparat penegak hukum, perlindungan hak asasi bagi warga negara, serta memperkuat sistem hukum nasional dalam menghadapi kejahatan digital yang terus berkembang. Reformulasi kebijakan ini juga merupakan manifestasi konkret dari fungsi negara dalam menjaga keamanan informasi, martabat individu, dan integritas ruang digital nasional.

B. Saran

Melihat belum adanya pengaturan yang tegas, sistematis, dan menyeluruh terhadap tindak pidana *doxing* dalam sistem hukum pidana Indonesia saat ini, disarankan agar pemerintah bersama pembentuk undang-undang melakukan reformulasi regulasi melalui revisi terhadap UU ITE dan UU PDP, serta

mempertimbangkan penyusunan undang-undang khusus tentang pelanggaran privasi berbasis teknologi. Revisi dan pembentukan regulasi tersebut harus secara eksplisit menyebutkan *doxing* sebagai tindak pidana yang berdiri sendiri, lengkap dengan unsur-unsur perbuatan, jenis-jenis *doxing* (seperti *targeting*, *delegitimizing*, dan *deanonymizing*), bentuk pertanggungjawaban pidana (*dolus* dan *culpa*), serta pengaturan sanksi yang proporsional berdasarkan dampak yang ditimbulkan. Langkah ini penting untuk menghindari multitafsir dan memperkuat efektivitas penegakan hukum di lapangan.

Selain penguatan aspek normatif, regulasi mendatang juga harus mengadopsi pendekatan yang komprehensif dengan mencakup tiga pilar utama: preventif, represif, dan rehabilitatif. Aspek preventif dapat diwujudkan melalui edukasi publik dan peningkatan literasi digital masyarakat terkait pentingnya menjaga kerahasiaan data pribadi. Aspek represif memuat ketentuan pidana yang adil dan proporsional terhadap pelaku *doxing* berdasarkan tingkat kesalahan dan dampaknya. Sedangkan aspek rehabilitatif harus memastikan bahwa korban mendapatkan hak atas pemulihan melalui pendampingan psikologis, perlindungan identitas, serta akses terhadap keadilan.

Bagi aparat penegak hukum, diperlukan penguatan kapasitas melalui pelatihan dan pembaruan pemahaman terhadap perkembangan kejahatan digital, khususnya *doxing*. Penegakan hukum tidak boleh hanya mengandalkan pendekatan formalistik, tetapi harus berbasis pada prinsip victim-oriented approach dan restorative justice, sebagaimana telah diterapkan dalam

Protection from Harassment Act (POHA) di Singapura. Dengan demikian, aparat dapat bertindak lebih cepat, sensitif terhadap kebutuhan korban, dan akurat dalam menerapkan sanksi terhadap pelaku.

Adapun bagi masyarakat, peningkatan kesadaran akan pentingnya perlindungan data pribadi dan risiko *doxing* harus menjadi bagian dari kebijakan publik. Pemerintah, lembaga pendidikan, dan platform digital harus berperan aktif dalam melakukan kampanye literasi digital dan penyuluhan hukum secara berkelanjutan. Masyarakat perlu didorong untuk bersikap lebih bijak dalam membagikan informasi pribadi secara daring, serta diberi pemahaman tentang hak-haknya sebagai subjek data dan jalur hukum yang tersedia apabila menjadi korban *doxing*.

Melalui sinergi antara regulasi yang progresif, kapasitas penegakan hukum yang memadai, dan kesadaran hukum masyarakat yang tinggi, Indonesia dapat membangun sistem perlindungan hukum yang adaptif dan efektif terhadap ancaman kejahatan siber, khususnya *doxing*, dalam era digital yang terus berkembang.